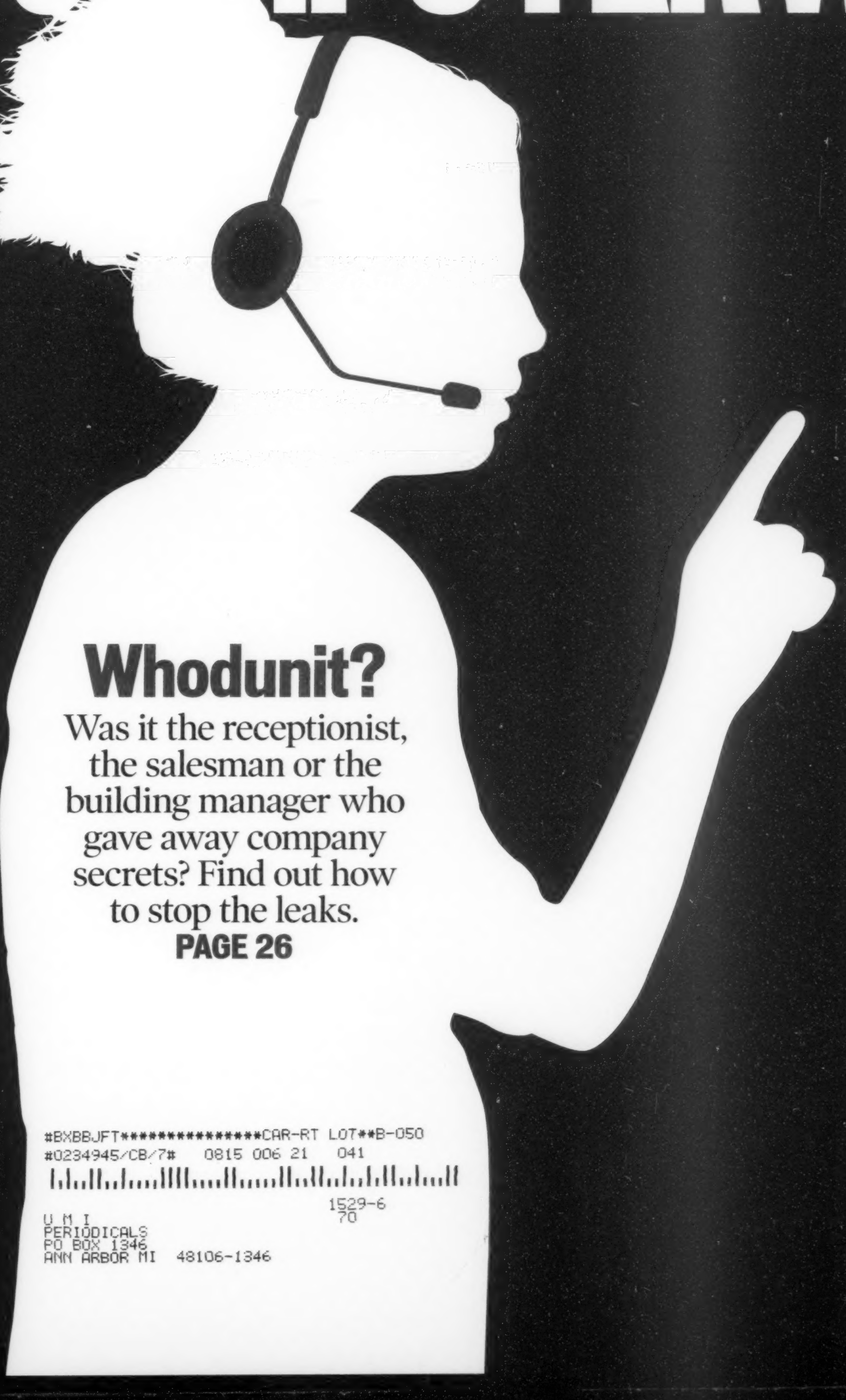
THE GRILL: Google enterprise product guru Matthew Glotzbach answers the question: What's so good about cloud computing? **PAGE 20**

COMPUTERWORLD®



Whodunit?

Was it the receptionist, the salesman or the building manager who gave away company secrets? Find out how to stop the leaks.
PAGE 26

#BXBBJFT***************CAR-RT LOT**B-050
#0234945/CB/7#   0815 006 21   041
1529-6
70
U M I
PERIODICALS
PO BOX 1346
ANN ARBOR MI 48106-1346

Inside

APRIL 14, 2008
VOL. 42, NO. 16 $5/COPY

News Analysis

Recent thefts of card data during electronic transmission raise questions about the PCI security standard's effectiveness. PAGE 16

IT executives are in a battle for control as business units again demand to make purchasing decisions on their own. PAGE 18

Opinions

'XP Lite' could be a smart mobile strategy for Microsoft. PAGE 24

Your information security squad is much bigger than you think. PAGE 44

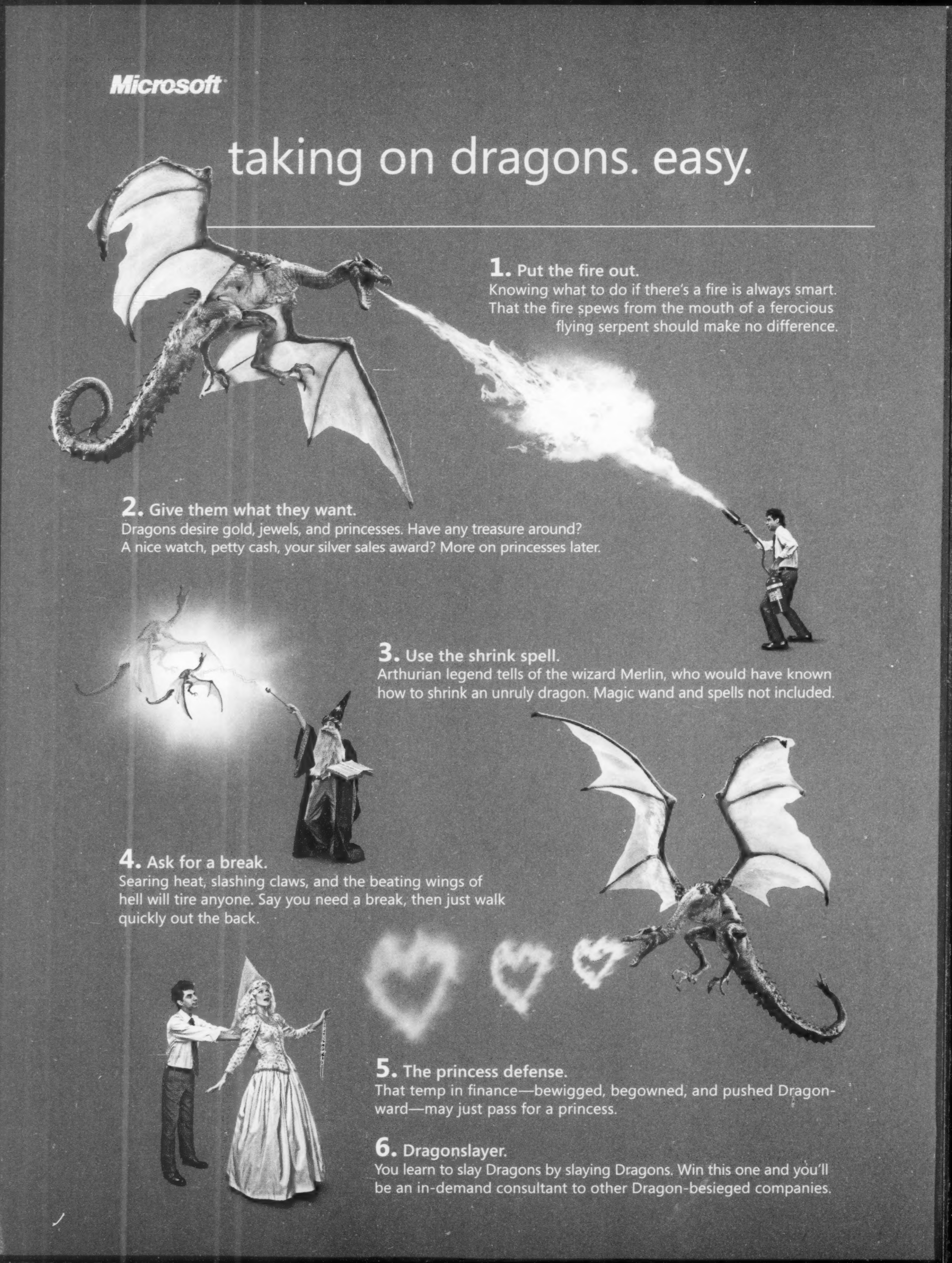
Careers

What's the single most important IT skill? The answer may surprise you. PAGE 40

Don't Miss

ON THE MARK: **SaaS offers a cure for boring IT applications.** PAGE 19

COMPUTERWORLD.COM



Microsoft

taking on dragons. easy.

1. Put the fire out.
Knowing what to do if there's a fire is always smart. That the fire spews from the mouth of a ferocious flying serpent should make no difference.

2. Give them what they want.
Dragons desire gold, jewels, and princesses. Have any treasure around? A nice watch, petty cash, your silver sales award? More on princesses later.

3. Use the shrink spell.
Arthurian legend tells of the wizard Merlin, who would have known how to shrink an unruly dragon. Magic wand and spells not included.

4. Ask for a break.
Searing heat, slashing claws, and the beating wings of hell will tire anyone. Say you need a break, then just walk quickly out the back.

5. The princess defense.
That temp in finance—bewigged, begowned, and pushed Dragonward—may just pass for a princess.

6. Dragonslayer.
You learn to slay Dragons by slaying Dragons. Win this one and you'll be an in-demand consultant to other Dragon-besieged companies.

taking on security threats. easier.

1. **Implement Microsoft® Forefront.™**
Forefront makes defending your systems easier. It's a comprehensive, simple-to-use, integrated family of products that helps provide protection across your client, server, and network edge. Learn how Del Monte Foods uses the Forefront family of products to help defend their systems. Visit **easyeasier.com**

Forefront is business security software for client, server, and the network edge.

Microsoft®
Forefront™

Inside

COMPUTERWORLD ■ APRIL 14, 2008

SPOTLIGHT | SECURITY

■ NEWS DIGEST

10 Cost and reliability concerns are keeping **storage buyers** away from **solid-state technology**. | An overflow of petitions requires a **lottery** to determine the 2009 **H-1B visa winners**.

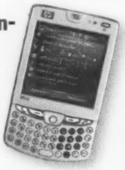
12 Analysts warn that **IT managers** must prepare for **cutbacks** now in the face of the **declining economy**. | **IBM** says its new **water-cooled server** will blunt IT energy concerns.

14 Apple's decision to push its **Safari browser** to incautious PC users as part of an iTunes and QuickTime update has **infuriated companies** now trying to remove the unwanted software.

■ NEWS ANALYSIS

16 Hackers Open New Front in Card Data Thefts. Recent thefts of credit and debit card data while in transit between systems are raising questions about whether the PCI security standard is fully equipping companies to fend off cybercrooks.

18 IT Keeps Battling to Maintain Control of Technology. Analysts and users say that business units are once again trying to wrest control of technology decisions away from IT.



■ OPINIONS AND FEATURES

8 Editor's Note: Don Tennant worries that students are getting the message that companies won't hire new grads, which could cause the pool of homegrown talent to dry up.

19 On the Mark: Mark Hall discovers that SaaS billing services, once unthinkable to CFOs, are already here.

20 The Grill: Matthew Glotzbach, Google's enterprise product guru, talks about the logic of cloud computing, corporate social networking and the advent of true utility computing.

24 Michael Gartenberg customized XP for a tiny laptop, which gave him an idea for Microsoft.

40 Career Watch: A *Computerworld* Premier 100 IT Leader discusses trust, and youth vs. experience.

42 Shark Tank: The network is completely down, but the mystery clears up when a user remembers that, oh yeah, he did do one little thing.

44 Frankly Speaking: Frank Hayes suggests that your information security squad should be much bigger than you think.

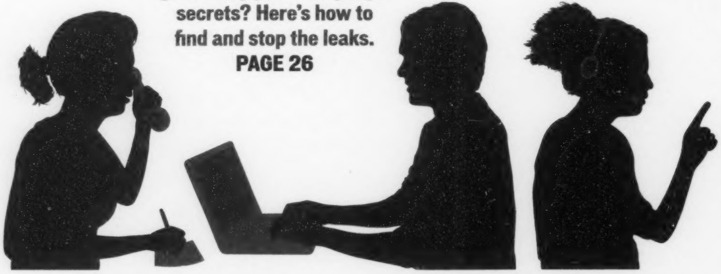
■ ALSO IN THIS ISSUE

Letters 9
Company Index 42

Whodunit?

» SPECIAL REPORT «

Was it the receptionist, the salesman or the building manager who gave away your company's secrets? Here's how to find and stop the leaks.
PAGE 26



28 Five Things Your HR People Should Know. Your human resources group handles – and shares – huge stores of sensitive data. This is a department in need of strict data-retention policies.

30 Five Things Your Salespeople Should Know. Your top salespeople are closing deals from coast to coast, yet they could be leaving a trail of data behind them. Here's how to make sure they're protecting the company's assets.

32 Five Things Your Receptionist Should Know. Your receptionist can weaken your company's security by falling for scams or illegally downloading files. Tighten up your front-line defense with targeted training.

33 Four Things Your Administrative Staff Should Know. Your administrative employees are just one step away from top executives and often have high-level data access. Here's how to keep that data safe.

34 Three Things Your Facilities Group Should Know. Your facilities managers literally hold the keys to your company's physical security. With some targeted training and standard practices, your building can be made a whole lot more secure.

34 Four Things Your Remote Staff Should Know. Your telecommuters and branch workers are out there in the ether – along with your company's equipment and data. Keep their unique security issues front and center.

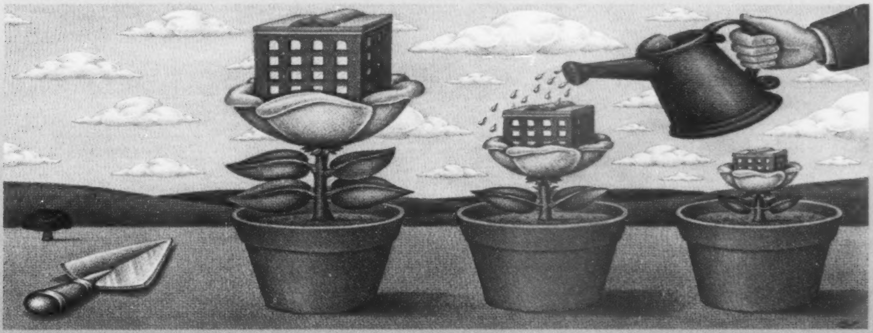
36 How to Spot a Spy. Con artists make it their job to extract sensitive corporate intelligence from unsuspecting employees. Here's how to stop them.

39 Opinion: Librarians have done battle with the government to protect their patrons' privacy. Columnist Mark Hall asks: How far will you go to defend the privacy of your customers' and employees' personal data?

COVER ILLUSTRATION BY BRANDON LAUFENBERG.

Innovations by **InterSystems**

Embed the ability to scale.



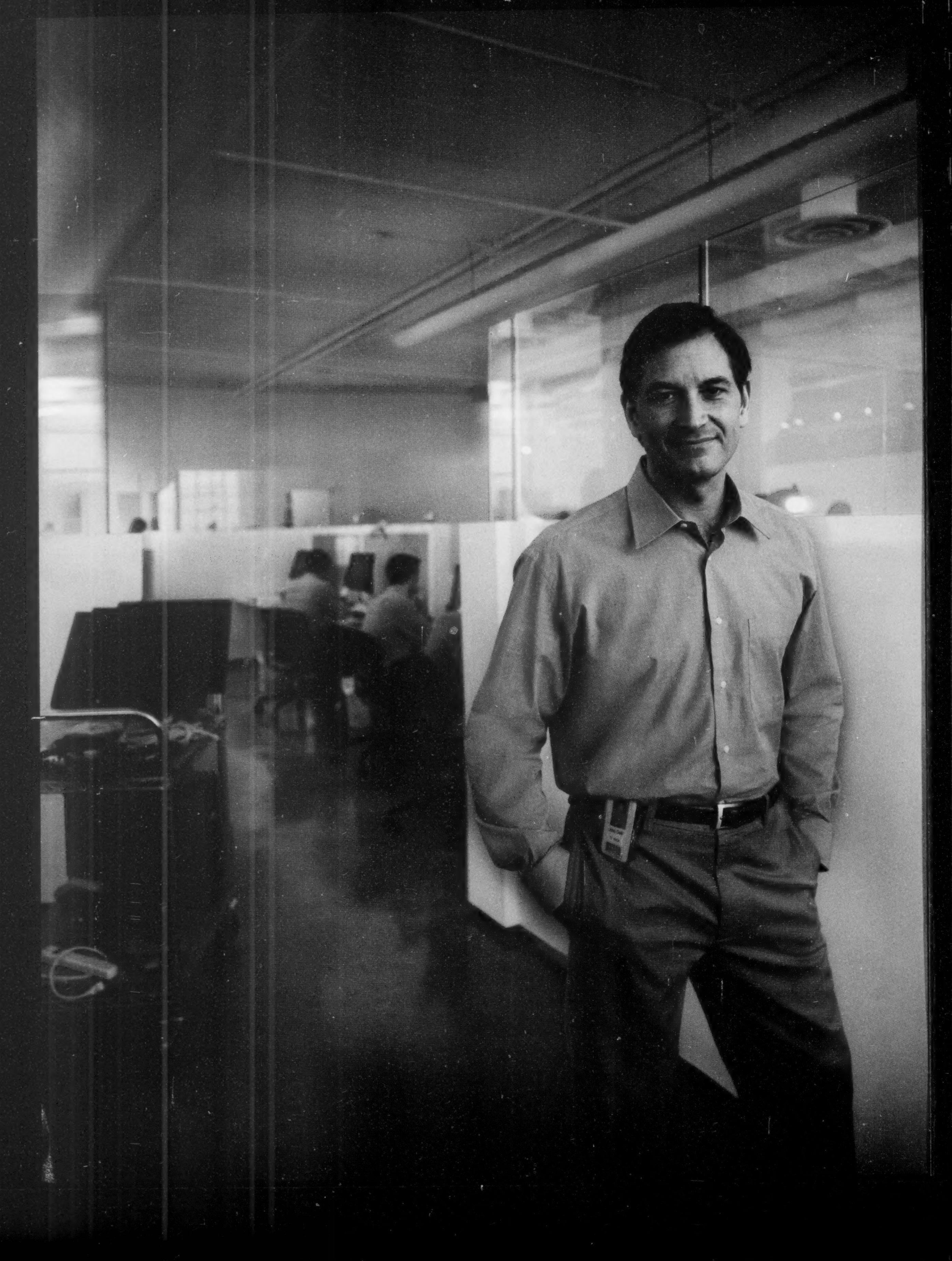
For software developers seeking competitive advantages, InterSystems Caché® makes applications more valuable by increasing their speed and scalability, while decreasing hardware and administration requirements. Embed our post-relational database in your applications, and enjoy the combined benefits of high-performance object and relational technologies. Thanks to its innovative architecture, Caché spares Java and .NET programmers a lot of tedious work by eliminating the need for object-relational mapping. Caché is available for Unix, Linux, Windows, Mac OS X, and Open VMS – and it supports MultiValue development. Caché is deployed on more than 100,000 systems worldwide, ranging from two to over 50,000 users. Embed our innovations, enrich your applications.

InterSystems CACHÉ®

Make Applications More Valuable

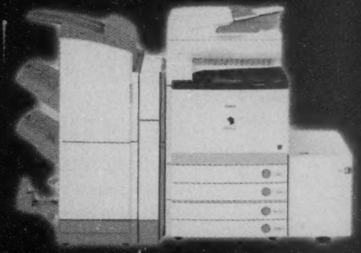
Download a free, fully functional, no-time-limit copy of Caché, or request it on CD, at **InterSystems.com/Cache26A**

© 2008 InterSystems Corporation. All rights reserved. InterSystems Caché is a registered trademark of InterSystems Corporation. 1-08 EmbedCache26 CoWo



IN THE WORLD OF ENTERPRISE INTEGRATION

I need a solution that runs like clockwork or I run the risk of running a lot of stairs.



The Canon Color imageRUNNER

PRODUCE. PERSUADE. PERFORM. ON THE NETWORK.

Color imageRUNNER®

www.usa.canon.com 1-800-OK-CANON

Canon and IMAGERUNNER are registered trademarks of Canon Inc. in the United States and may also be registered trademarks or trademarks in other countries. IMAGEANYWARE is a trademark of Canon. © 2008 Canon U.S.A., Inc. All rights reserved. Product shown with optional accessories.

Canon

imageANYWARE

COMPUTERWORLD.COM

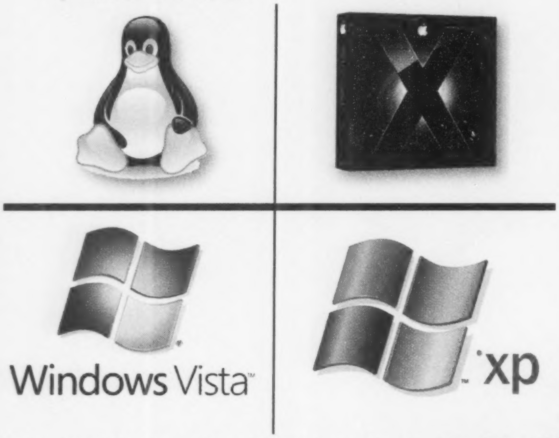
This Week Online

FIND THESE STORIES AT COMPUTERWORLD.COM/MORE

OS Smackdown:

Mac OS X vs. Windows Vista Vs. Linux vs. Windows XP

Forget market share – which desktop operating system is truly the best? Four experts defend their OS of choice in an opinionated free-for-all.



Review: Helping Smart-Phone Users Do Real Work

RedFly is a very smart implementation of a dumb terminal that will let smart-phone users get some real work done on the road without using a laptop.

Vendor Disk Failure Rates: Myth or Metric?

The vendors themselves acknowledge that "your mileage may vary." So how do their statistics help buyers?

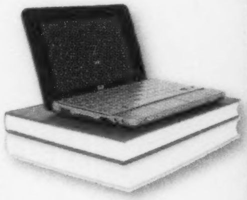
Mike Elgan: Why Not Give Users What They Want?

Vendors want us to buy amazing gadgets like super smart phones with video, Wi-Fi and 4G. But columnist Mike Elgan notes that too often, these amazing products are missing basic features.

A New Kind of Web – Don't Miss These 11 Sites

Check out these examples of how the Web is evolving to present information in new ways that can help you get organized, boost productivity or just have some fun.

Review: HP's 2133 Mini-Note Takes on the Eee PC



HP's new 2133 Mini-Note is a hair heavier and more expensive than the Eee PC, but its bright screen and sleek design will have broader appeal.

Will Microsoft Deliver Windows 7 Next Year?

Recent statements hint at the possible arrival of the next version of the operating system in 2009.

Blog Spotlight

The Ultimate Hotel-Room Finder

A Google Maps mashup called the Map Channels Hotels Directory shows all of the hotels in a particular locale, with availability listed in order of price. Blogger Mike Elgan wishes he'd known about it for his last trip.

Off the Grid

What's the one thing reporter Matt Hamblen didn't bring to Las Vegas for the CTIA convention on wireless technology? His cell phone. The ironic situation was manageable, though unnerving.

SHARK BAIT

But It Makes Sense!

It's simple math that a 21-in. monitor is bigger than a 15-in. one. One boss uses this logic and a measuring tape to complain that his company's internal applications won't fit on his screen.

ONLINE DEPARTMENTS

Breaking News	computerworld.com/news
Newsletter Subscriptions	computerworld.com/newsletters
Knowledge Centers	computerworld.com/topics

IBM

_INFRASTRUCTURE LOG

_DAY 62: Our power and cooling costs are out of control. We're spending the bulk of our IT budget just keeping the servers cool. I told Gil we need to go green in a big way.

_DAY 63: He took us green...kelly green, to be exact.

_DAY 64: I told Gil you don't go green with paint. You go green with the new IBM Power™ Systems. The Power 550 Express uses 91% less energy and 98% less space compared to a 64-core HP 9000 Superdome. And it gives us 16% more transaction performance running the UNIX® platform[1]...Wow.

_Our data center will be truly green now. And painted white.

Trade up your PA-RISC system with the IBM Power Rewards Program:[2]

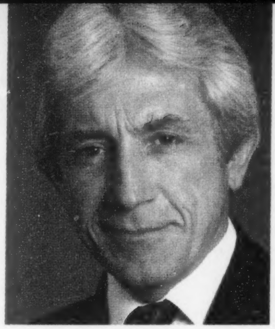
IBM.COM/**TAKEBACKCONTROL**/POWER

1. HP 9000 Superdome Enterprise server comparison utilizes 64 cores – 875 MHz PA-RISC 8700 processors 256 GB of memory. Power consumption figures of 1400W for the IBM Power 550 and 16,920W for the HP 9000 Superdome were based on the maximum rates published by IBM and HP, respectively. For complete details, go to ibm.com/takebackcontrol/benchmark.
2. U.S. offering on select models only. More information about this program can be obtained through ibm.com/products/us – enter SPECOFFSP in the NavCode® window. IBM, the IBM logo, Power and Take Back Control are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries. UNIX is a registered trademark of The Open Group in the United States and other countries. ©2008 IBM Corporation. All rights reserved.

■ EDITOR'S NOTE

Don Tennant

Pro or Parasite?



THERE ARE a lot of CIOs around who dismiss the idea of hiring graduates fresh out of college. I know, because I've spoken with many of them. They clearly have their reasons, and it would be foolish to claim that none of them are legitimate. But it seems like an awfully shortsighted approach to skills management.

Of all the issues we cover, none seems more volatile or emotional than the subject of IT skills and labor management, encompassing as it does issues like H-1B visas, offshore outsourcing and the debate over whether an IT labor shortage even exists. During a panel discussion on this topic at our Premier 100 IT Leaders Conference last month, we polled the audience to see whether attendees believed there is such a shortage. Forty-six percent said yes, 43% said no, and 11% said they weren't sure. I wasn't surprised to see the results so evenly split.

The lack of consensus extends to the question of whether the U.S. education system is producing enough graduates in technology-related fields. We've all read about the concern that the U.S. is losing its competitive edge because China, India and other countries are educating far more scientists and engineers than we are. But there's plenty of debate over whether that concern is legitimate.

For example, last November, Harold Salzman of the Urban Institute testified before Congress that research conducted in collaboration with Case Western Reserve University and Georgetown University found no shortage of STEM (science, technology, engineering and mathematics) graduates in the U.S.

"The available data indicate that the United States' education system produces a supply of qualified STEM graduates in much greater numbers than jobs available," Salzman testified. "If there are shortages, it is most likely a demand-side problem of STEM career opportunities that are less attractive than career opportunities in other fields."

What needs to be factored into the equation, however, is that a hefty percentage of those graduates are foreign nationals.

■ It's easy to dump the responsibility for hiring and training new graduates onto other companies. But there's something distastefully parasitic about that.

According to Salzman's report, in 2005, 38% of computer science and 42% of computer engineering graduates in master's degree programs were non-U.S. citizens. To the extent that the benefit of the knowledge gained by those foreign students lies outside of the U.S., it's clear that there's still a lot of work to be done to encourage young Americans to advance U.S. competitiveness by pursuing degrees in STEM disciplines.

What's equally clear is that if the message being sent to our young people is that companies will be reluctant to hire them when they graduate, they'll steer clear of technology, the pool of homegrown talent will dry up, and the question of whether there's an IT labor shortage will be far less debatable.

It's easy for a company to argue that its skills requirements can be met only by experienced workers, just as it's easy to dump the responsibility for hiring and training new graduates onto other companies. But there's something distastefully parasitic about that.

One company that has embraced its responsibility is Monsanto, the St. Louis-based agricultural giant. I was discussing the topic of IT labor last week with Monsanto's CIO, Mark Showers, who told me about the company's Cooperative Education Program. The program has existed for over 30 years but was revitalized in 2002 when Monsanto's IT organization took ownership of it.

University students are recruited into the program during their sophomore year, and during their junior and senior years they spend six months in school and six at Monsanto. According to Showers, the company ultimately hires 80% to 90% of those students. The program has been so successful, in fact, that Monsanto received the 2007 Employer of the Year Award from the Midwest Cooperative Education and Internship Association.

Monsanto is well known for producing pesticides to get rid of agricultural parasites. Now if only the example of professionalism it has set in the field of education could rid us of corporate parasites as well. ■

Don Tennant *is editorial director of* Computerworld *and* InfoWorld. *Contact him at don_tennant@computerworld.com, and visit his blog at http://blogs.computerworld.com/tennant.*

You Never Forget Your First Computer

Gary Anthes' comments about the 1401 brought back fond memories ["Tales From the Crypt: Our First Computers," *Computerworld.com*, March 25]. I started out wiring boards on 407 tab equipment, then moved up to a 1401G (a 4k machine). My first application was a mortgage loan system for 12 banks. I learned a lot about overlays and coding in "actual."

Forty-three years later, I'm still at it, only now I get to play with everything from embedded systems to supercomputers. Having experienced working so intimately with the hardware at the beginning still provides valuable insight into what's going on through all the layers of fog in today's technology. When you think about it, a cell phone is now more powerful than the most powerful computer of not that many years ago.

■ **Richard Bender,** *president, Bender RBT Inc., Queensbury, N.Y., rbender@BenderRBT.com*

Let's Recognize How Critical Training Is

For some time, I have been consistently facing the issue of there not being enough qualified IT workers available in the market ["Retraining Dilemma," Editor's Note, March 24]. I find the same as I broach the subject with my colleagues.

I agree 100% that companies need to step up to the plate and help retrain their IT employees. I find too often that IT's training budget is the first to be slashed while other "profit-generating" departments are increased. IT is just as important to the bottom line and strategy.

■ **Jesus V. Arriaga,** *CIO, Bosley, Los Angeles, arriagaj@yahoo.com*

As long as I can remember, training has been treated as a perk, something to be lavished on those who have time rather than a targeted method for a team or the corporate culture. I recall that much of the training given to me and my colleagues went to waste, since people had no way to use the new techniques once they returned to work. A few people, the ones who really got it, sometimes left the organization to seek a place where they really could improve the way they worked and developed software.

Today, the fat training budgets are gone, and so are the days of training your own staff. Those of us with corporate knowledge are cast aside in favor of cheaper (often foreign) labor that brings some specific technical skill. As for the methods of the past, these newbies just hack away in higher-level languages, but the theme remains the same. The MIPS are cheaper; the people are cheaper; but the quality of our industry has made little progress overall.

■ **Jason Martin,** *consultant, St. Augustine, Fla., CaptJason@aol.com*

'Touch-Screen Voting Made Me Feel Better'

The key thing to me when it comes to touch-screen voting is that asking voters if they trust the machine misses the point ["Voters Trust Touch-Screen Machines, Studies Show," *Computerworld.com*, March 26]. Do you ask patients whether a medical test is accurate, or do you ask the doctors who look at the results? Patients will tell you who treated them with consideration, whether the test was uncomfortable, who explained what was going on, etc. But you'll have no clue whether the test gave the right result.

It's unfortunate that professor Paul Herrnson and his colleagues haven't understood this basic concept. I'm glad that the headline in *Computerworld* clarifies that voters are making the judgment (and not experts), but it's unfortunate that such pseudo-science is getting widespread publicity.

■ **Jeremy Epstein,** *senior security consultant, Cyber Defense Agency LLC, Fairfax, Va.*

COMPUTERWORLD
P.O. Box 9171, 1 Speen Street
Framingham, MA 01701
(508) 879-0700
Computerworld.com

■ **EDITORIAL**
Editorial Director Don Tennant
Editor in Chief Scot Finnie
Executive Editors Mitch Betts, Julia King (events)
Managing Editors Michele Lee DeFilippo (production), Sharon Machlis (online), Ken Mingis (news)
Design Director Stephanie Faucher
Features Editors Kathleen Melymuka, Valerie Potter, Ellen Fanning (special reports), Barbara Krasnoff (reviews)
Senior Editor Johanna Ambrosio (channels)
Senior News Editor Craig Stedman
News Editors Mike Bucken, Marian Prokop
National Correspondents Gary Anthes, Thomas Hoffman, Julia King, Robert L. Mitchell
Reporters Brian Fonseca, Sharon Gaudin, Matt Hamblen, Heather Havenstein, Gregg Keizer, Eric Lai, Linda Rosencrance, Patrick Thibodeau, Jaikumar Vijayan, Todd R. Weiss
E-mail Newsletters Editor David Ramel
Channel Editors Johanna Ambrosio (servers and data centers), Angela Gunn (security), Lucas Mearian (storage), David Ramel (networking and Internet)
Assistant Managing Editor Bob Rawson (production)
Blogs and Projects Editor Joyce Carpenter
Editor at Large Mark Hall
Senior News Columnist Frank Hayes
Art Director April O'Connor
Associate Art Director Owen Edwards
Research Manager Mari Keefe
Senior Copy Editors Eugene Demaitre, Monica Sambataro
Copy Editor Donna Sussman
Associate Editor, Community Ken Gagné
Office Manager Linda Gorgone
Contributing Editors Jamie Eckle, Preston Gralla, David Haskin

■ **CONTACTS**
Phone numbers, e-mail addresses and reporters' beats are available online at *Computerworld.com* (see Contacts link at the bottom of the home page).
Letters to the Editor Send to letters@computerworld.com. Include an address and phone number for immediate verification. Letters will be edited for brevity and clarity.
24-hour news tip hot line (508) 620-7716
Subscriptions and back issues (888) 559-7327, cw@omeda.com
Reprints/permissions The YGS Group, (800) 290-5460, ext. 150, computerworld@theygsgroup.com

News Digest

FIND THE FULL STORIES AT
COMPUTERWORLD.COM

THE WEEK AHEAD

MONDAY: Collaborate '08, a conference jointly run by three Oracle user groups, begins in Denver. Also starting today are Microsoft's MVP Global Summit in Seattle and the MySQL Conference & Expo 2008 in Santa Clara, Calif.

TUESDAY: The IT Business Excellence Forum opens in Orlando, featuring the CIOs of AutoZone and Best Buy.

THURSDAY: Advanced Micro Devices is due to report its Q1 financial results, with revenue below expectations.

More than 2,000 people attended Storage Networking World last week.

ANDY MENG

STORAGE

Solid-State Drives Still Not Ready for IT, Users Say

ORLANDO

SOLID-STATE storage technology may offer some performance advantages, but for most companies, it remains too costly and unreliable for data center use, said several attendees here at last week's Storage Networking World conference, which was co-sponsored by *Computerworld* and the Storage Networking Industry Association.

Gregory Gum, an engineering specialist at The Aerospace Corp., called the nascent drives "a bit scary" compared with hard drives.

"It's still a niche technology," he said. "[It's] expensive and always will be."

Gum predicted that it will take at least five years for solid-state memory to be widely deployed.

Rick Coulson, a senior fellow at Intel Corp., warned IT managers to be wary of the technology. "You have to have a performance reason for solid-state drives to make sense," Coulson said. "I wouldn't recommend them if you care about dollars per gigabyte. [But] if you care about dollars per unit of performance, that's different."

"I wouldn't recommend [solid-state drives] if you care about dollars per gigabyte. [But] if you care about dollars per unit of performance, that's different.

RICK COULSON,
SENIOR FELLOW, INTEL CORP.

He said solid-state technology is best suited for applications that require high throughput and for high-performance software like transactional databases and Web services.

Companies that don't need the performance see no need to switch from hard drives. "We're not splitting atoms . . . so that's not a big consideration," said Ed Richard, an IT infrastructure engineer at Stiefel Laboratories Inc. "Am I going to put [a solid-state disk] into a SQL database? Absolutely not."

Richard is interested in the technology's promise of minimizing cooling and maintenance costs but said its limited storage density would need to be addressed.

"Our [system capacity] has to scale up to 1 petabyte," he said. "I can't imagine the number of [flash] drives you would need to make up for that."

Jeffrey Janukowicz, an analyst at IDC, said corporate users will hold off on adopting solid-state storage until the second generation of the drives emerges next year.

— Brian Fonseca

IMMIGRATION

Lottery Will Select H-1B Winners

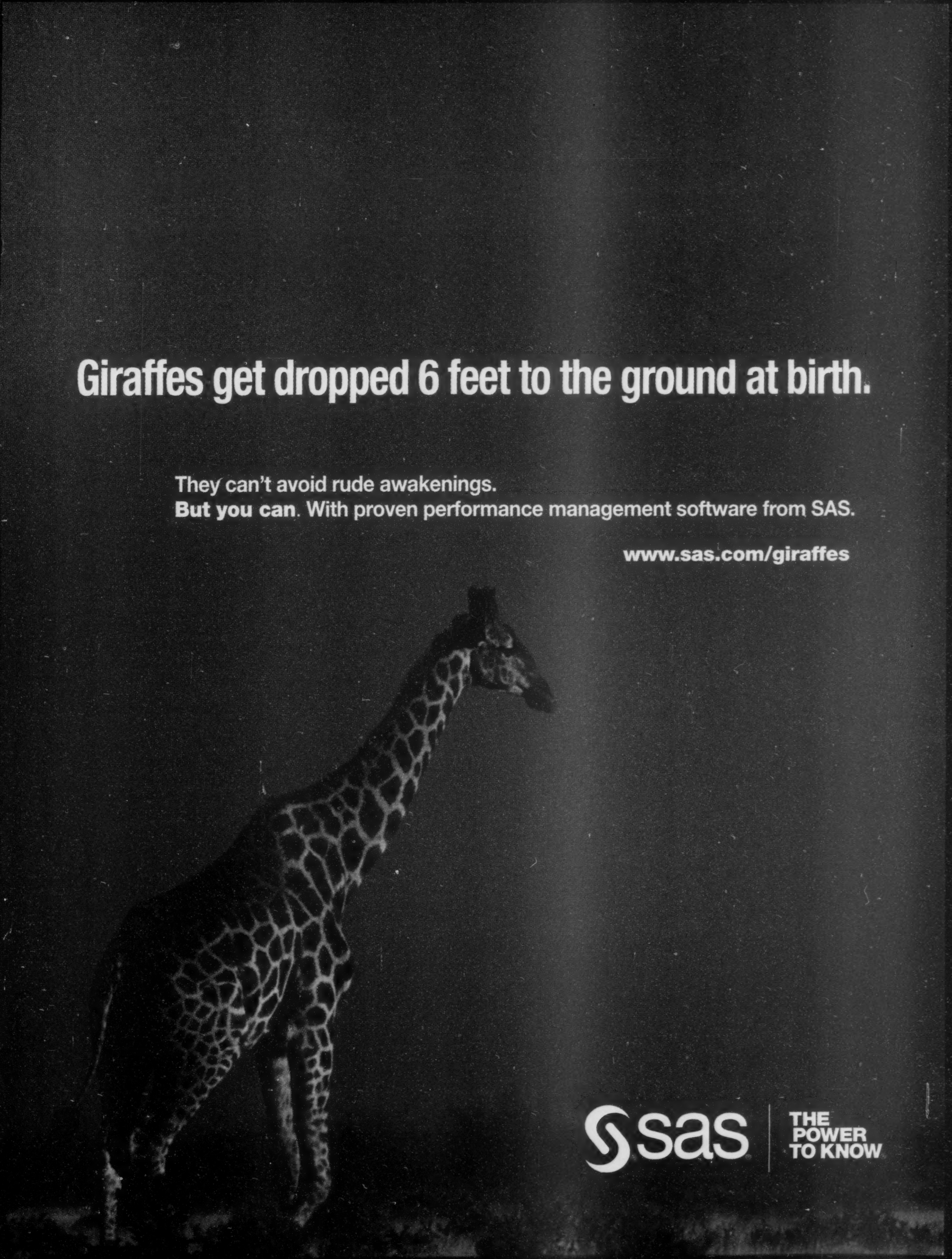
The U.S. government last week announced that H-1B visas for fiscal 2009 will be issued via lottery, after employers submitted another overflow batch of petitions earlier this month.

U.S. Citizenship and Immigration Services received 163,000 requests for H-1B visas – a record number requiring the use of a computerized random-selection process. The requests were made to the agency, which is part of the U.S. Department of Homeland Security, during a five-day filing period that started on April 1. Last year, there were 143,000 petitions for 85,000 available visas.

This year, the USCIS will issue 65,000 regular visas and 20,000 more for foreign nationals with advanced degrees from U.S. universities.

The DHS extended from 12 months to 29 the period that foreign graduates of U.S. universities can hold jobs in the U.S. without work visas.

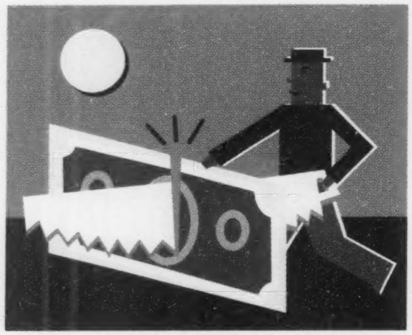
– PATRICK THIBODEAU



Giraffes get dropped 6 feet to the ground at birth.
They can't avoid rude awakenings.
But you can. With proven performance management software from SAS.
www.sas.com/giraffes
sas
THE POWER TO KNOW

MANAGEMENT

IT Execs Warned to Get Ready for Rapid Cutbacks


GETTY IMAGES

LAS VEGAS

THE IT cost-cutting phase of the current economic downturn may arrive like a buzzsaw — with force and immediacy, Gartner Inc. analysts warned data center managers at the research firm's Symposium/ITxpo conference here last week.

In fact, said Gartner analyst Ellen Kitzis, IT managers will likely have as little as a few weeks to act on financial directives from top corporate executives.

Mike Lyon, assistant vice president for computer operations at the University of Illinois at Urbana-Champaign, agreed that planning for possible cutbacks should "start now."

"CEOs are probably going to give us two weeks, if we're lucky, to come up with a well thought-out plan," Lyon said.

Kitzis suggested that in addition to preparing for traditional cost-cutting measures like freezing head counts, IT managers should look for new ways to reduce costs. For example, management layers could be cut as part of a larger effort to adapt to emerging collaborative work models.

Clint Hubbard, CIO for the city of Albuquerque, is already working to flatten his organization and has implemented a hiring freeze to cut costs.

Hubbard acknowledged that cutting management posts — increasing the number of workers who report to each manager — will probably hurt productivity. "I will get something less than what I'm used to, but that's the only option," he added.

Gartner analyst William Snyder suggested that before reducing personnel, IT managers should implement simpler measures, such as closely scrutinizing invoices. "Make sure you are getting charged the right price," he advised.

He also said businesses can cut IT costs by getting rid of unused software and by making sure old products are retired when new ones are installed. And when it comes to negotiations, customers may strike better deals by waiting for the last days of a vendor's fiscal quarter, he noted.

Analyst Phillip Redman added that using expense management services and eliminating unused phones that are still accruing monthly charges could cut telecom costs by 10% to 35%.

— Patrick Thibodeau

Short Takes

Oracle Corp. this week plans to release 41 software patches, including fixes for two bugs in its flagship database that can be exploited over a network without a username and password. The company will also issue 11 patches for its E-Business Suite applications.

Symantec Corp. has agreed to purchase **AppStream Inc.**, a maker of desktop virtualization software, for an undisclosed sum. Symantec has been reselling AppStream's software with its Software Virtualization Solution Pro product since 2006. The deal is expected to close in June.

IBM has agreed to buy **FilesX Inc.**, a Haifa, Israel-based maker of storage software. Terms were not revealed. The FilesX products will become part of IBM's Tivoli line when the deal closes.

Advanced Micro Devices Inc. has started shipping its quad-core Opteron processor, code-named Barcelona, after a delay of several months to fix a bug discovered last fall.

HARDWARE

IBM Unveils Water-Cooled Supercomputer

IBM LAST WEEK unveiled a still-rare water-cooled server as part of an effort to help companies wrestling with a lack of data center power.

The Power 575 supercomputer incorporates the company's new Hydro Cluster design, which includes a network of copper pipes that carry cold water to the system's processor and warm water away from it.

Water cooling is more efficient than air cooling – 4,000 times more efficient, according to IBM – and it allows the company to cram 448 4.7-GHz Power6 processor cores into a Power 575 rack, said Scott Handy, vice president of worldwide marketing and strategy.

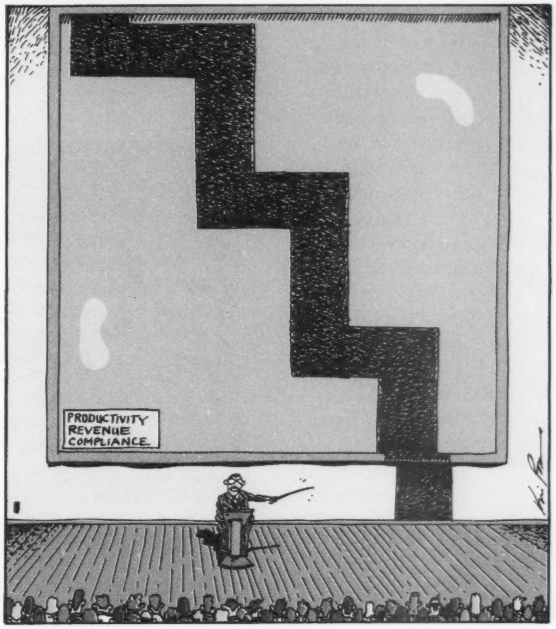
Independent analyst Joe Clabby said that water-cooled systems had fallen out of favor in recent years because of the hassle of setting them up. But air conditioning costs have risen to a point where water cooling again makes sense, he said.

Handy declined to say if other Power systems will use the water-cooling technology, but "we are definitely saying that water will be used more in future in the data center," he noted.

IBM also upgraded its high-end air-cooled Unix-based supercomputer, the Power 595, with a new Power 6 processor that runs at up to 5 GHz. Both it and the Power 575 will ship next month.

– JAMES NICCOLAI,
IDG NEWS SERVICE

IBM's Hydro Cluster technology brings cold water directly to the hottest part of the chip.



© 2008 JUNIPER NETWORKS, INC.

"Currently, our network can't keep up with the growing electronic data demands, which causes revenue and productivity to... if you'd all like to follow me down a floor, I'll continue."

>> **Business demands bringing you down?** Then trust the Juniper Networks portfolio of network infrastructure solutions to keep you ahead of constantly evolving business requirements. Juniper delivers more choice and control from your network, while our streamlined JUNOS™ software minimizes downtime and reduces complexity, network management expenses and operating costs.

Increase the value of your network by bringing innovation to market faster. That's a clear competitive edge. The switch is on to high-performance network infrastructure: **www.juniper.net/connected**

Juniper your Net™

1.888.JUNIPER

INTERNET

Uninvited Guest – Safari – Hits Corporate Networks

APPLE INC.'S push to offer its Safari Web browser as part of a mid-March iTunes and QuickTime update is forcing some corporate network administrators to work quickly to remove the software from enterprise PCs.

Cody Wilson, a network administrator at Soy Capital Bank and Trust Co. in Decatur, Ill., said that soon after the update was posted, he found that some users on the bank's network had installed the software without realizing it.

"I scanned my network, and my inventory software said I have Safari on 30 PCs," he said.

Apple had configured the update so that users who clicked "OK" on a pop-up message would automatically install its Web browser on their PCs. Most users thought that Safari was simply a component of the Apple software they had already installed, Wilson said.

"This is not good; this is a security risk," Wilson said. "We're a bank."

Wilson said it took almost a week to remove Safari from his network and to prevent it from being reinstalled.

Susan Bradley, chief technology officer at Tamiyasu, Smith, Horn and Braun Accountancy Corp. in Fresno, Calif., said the updates are creating problem for administrators and could cause security risks if installed on corporate PCs.

"It impacts all of us when more potential attack surface is installed in a group of folks that are vulnerable enough as it is," she said.

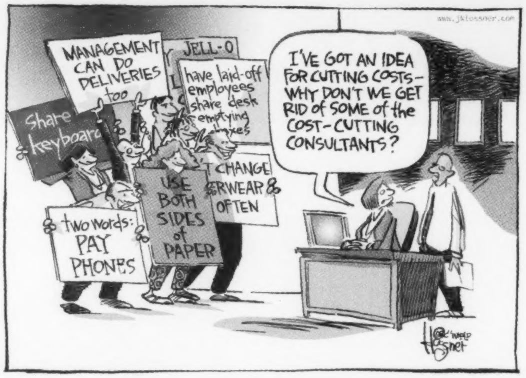
Bradley said that a user who patches corporate systems for her firm's IT unit inadvertently downloaded Safari when installing the QuickTime update.

Earlier this month, Shavlik Technologies LLC updated its Shavlik NetChk Protect software so it can detect and remove Safari from PCs, said Eric Schultze, CTO at the Roseville, Minn.-based security vendor.

— Robert McMillan, IDG News Service

BETWEEN THE LINES

By John Klossner


www.jklossner.com
MANAGEMENT CAN DO DELIVERIES too
JELL-O
have laid-off employees share desk emptying boxes
Share keyboard
two words: PAY PHONES
USE BOTH SIDES of PAPER
CHANGE RWEAR & OFTEN
I'VE GOT AN IDEA FOR CUTTING COSTS – WHY DON'T WE GET RID OF SOME OF the COST-CUTTING CONSULTANTS?
C'WORLD Klossner

BENCHMARKS LAST WEEK

Iomega Corp. accepted **EMC Corp.**'s latest buyout offer of $213 million, after spurning previous hostile offers of $178 million and $205 million.

Advanced Micro Devices Inc. announced plans to lay off 10% of its workforce, or about 1,600 employees, by the third quarter of 2008 in an effort to cut costs and return to profitability.

44 YEARS AGO: IBM launched its System/360 mainframe line, the first family of computers that could continue running the same software as new models were added.

Global Dispatches

Asustek Sues IBM In Patent Dispute

TAIPEI – Motherboard maker Asustek Computer Inc. earlier this month filed a lawsuit in U.S. federal court charging that IBM has infringed on two of its patents.

The suit was filed four months after the U.S. International Trade Commission agreed to investigate IBM's claims that Asustek had violated three of its patents.

Asustek alleges that IBM has infringed on patents related to its storage-area networking equipment and server products.

Asustek is seeking undisclosed monetary damages and wants to halt IBM's alleged use of the patented technology.

Asustek, which is based here, declined to comment on the lawsuit. IBM officials could not be reached.

Dan Nystedt,
IDG News Service

Microsoft Expands Health IT Efforts

BERLIN – Microsoft Corp. last week announced at the CohnIT heath care show here that it has started distributing its Amalga health care software in Europe.

Microsoft bought the software, which is used to manage data in various health care accounting systems, in 2006 from Datomics Licensing and General Datomics, as part of an effort to enter new markets.

Tola Sargeant, an analyst at London-based Ovum Ltd., said the Microsoft offering could successfully compete with products from European health care software makers.

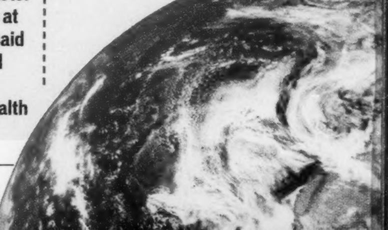
"If it can be proven in widescale deployments, Amalga is likely to have strong appeal for European health care providers, particularly those with a mishmash of clinical and departmental systems," Sargeant wrote in a research note.

Jeremy Kirk,
IDG News Service

BRIEFLY NOTED

Yahoo Inc. last week agreed to buy almost all of the assets – including Web analytics tools and an R&D operation – of Tensa Kft in Budapest. Terms of the deal, expected to close by mid-2008, were not disclosed.

Linda Rosencrance
Computerworld

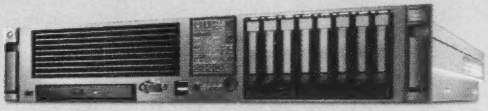


ALTERNATIVE THINKING ABOUT SERVER MANAGEMENT:

You don't have to be in your server room to manage your servers.

The HP ProLiant DL385 G5 Server, featuring efficient Quad-Core AMD Opteron™ processors, lets you manage it from your office in San Diego while it sits in Boston. Remote Management (iLO2) lets you control, reboot and troubleshoot from practically anywhere, even when the server is off.

Technology for better business outcomes.



HP ProLiant DL385 G5

$2525 (Save $1420)

Lease for as low as $63/mo[1] for 48 months

Smart Buy (PN: 464211-005)

- 2 Quad-Core AMD Opteron™ processors
- Supports small form factor, high-performance SAS or low-cost SATA hard drives
- Redundant Power
- Integrated Lights-Out (iLO2), Systems Insight Manager, SmartStart

Get More:

Smart Buy 24x7, 4 hour response, 3 years (PN: UE894E) $689

Smart Buy Add 2 GB additional memory (PN: 408851-S21) $159

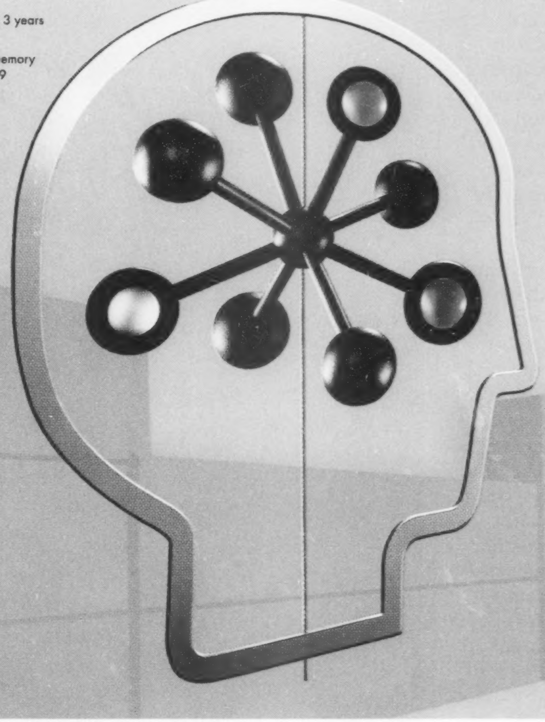
HP StorageWorks Ultrium 448 Tape Drive SAS Bundle

$1649

Lease for as low as $41/mo[1] for 48 months

Smart Buy (PN: AG739A)

- 400 GB compressed capacity in half-height form factor
- Ships with Data Protector Express Software, One Button Disaster Recovery, a 1U Rackmount Kit, and a Host Bus Adapter



10,000,000 I.T. folks can't be wrong.

To learn more, call 1-888-220-7138 or visit hp.com/go/dependable14

Prices shown are HP Direct prices; reseller and retail prices may vary. Prices shown are subject to change and do not include applicable state and local taxes or shipping to recipient's address. Offers cannot be combined with any other offer or discount and are good while supplies last. All featured offers available in U.S. only. Savings based on HP published list price of configure-to-order equivalent ($3945 - $1420 instant savings = SmartBuy price of $2,525). 1. Financing available through Hewlett-Packard Financial Services Company (HPFS) to qualified commercial customers in the U.S. and subject to credit approval and execution of standard HPFS documentation. Prices shown are based on a lease of 48 months in terms with a fair market value purchase option at the end of the term. Rates based on an original transaction size between $3,000 and $25,000. Other rates apply for other terms and transaction sizes. Financing available on transactions greater than $349 through July 31, 2008. HPFS reserves the right to change or cancel these programs at any time without notice. AMD, the AMD Arrow logo, AMD Opteron, and combinations thereof are trademarks of Advanced Micro Devices, Inc. © 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Hackers Open New Front in Card Data Thefts

Cybercrooks are stealing info while it's in transit between systems. Can the PCI rules stop them? **By Jaikumar Vijayan**

SECURITY managers often describe their efforts to protect corporate data from being compromised as a full-fledged battle of wits against cybercrooks who are continually arming themselves with innovative tools and methods of attack.

And the security breaches disclosed last month by Hannaford Bros. Co. and Okemo Mountain Resort — along with unconfirmed reports of dozens of similar network intrusions — suggest that a new front may have opened up in the battle.

Perhaps even more alarming, the recent incidents call into question whether the payment card industry's highly publicized data security standards are fully equipping companies to fend off attackers.

What's noteworthy about the Hannaford and Okemo breaches is that they both involved the theft of data in transit — credit and debit card information that was being transmitted from point-of-sale systems to payment processors in order to authorize transactions.

ISTOCKPHOTO

In Hannaford's case, the Scarborough, Maine-based supermarket chain has said that malware planted on the servers at about 300 grocery stores in the Northeast and Florida intercepted up to 4.2 million credit and debit card numbers and periodically sent the data in batches to a system overseas.

Just two weeks after Hannaford disclosed its breach, Okemo reported that data from more than 46,000 payment card transactions may have been compromised during a 16-day system intrusion in February.

Some of the data that was stolen was from transactions that occurred two years ago, but data from purchases made by customers while the intrusion was taking place appears to have been stolen in real time during the authorization and card-verification process, according to a spokeswoman for the Ludlow, Vt., ski area.

"The information was being taken as the cards were being swiped," she said, adding that law enforcement officials have told Okemo's management that they are investigating about 50 such incidents in the Northeast alone.

If that is indeed the case, it indicates that malicious hackers are starting to focus on stealing card data while it's on the move, instead of trying to take information that's stored on systems.

Ironically, the push by attackers to get at data in transit is likely a direct response to retailers' efforts to implement the security controls mandated by the Payment Card Industry Data Security Standard, or PCI for short, said Gartner Inc. analyst Avivah Litan.

The PCI standard, which was created by the major credit card companies, prohibits retailers and other merchants from storing payment card data on their systems in most cases, and it requires them to encrypt the data that they are allowed to store. Litan said that as more companies comply with the standard, credit card thieves are being forced to turn their attention away from the databases that they previously had targeted.

And the apparent success of the intruders who broke into the systems at Hannaford and Okemo is bound to embolden other attackers to try the same kind of strategies, Litan warned.

PCI WEAKNESSES?

The Hannaford breach, at least, points to possible holes in the PCI defense wall. The grocer has said that it was certified as being compliant with the security standard last year and then again on Feb. 27. That was the day Hannaford was first made aware of suspicious activity involving the credit cards of its customers.

The PCI rules require merchants to encrypt sensitive data while it's being transmitted across open public networks that attackers could easily use to intercept and divert information. But they aren't required to encrypt payment card information while it's in transit on their internal networks.

Bob Russo, general manager of the PCI Security Standards Council, said last week that there isn't enough information available about the Hannaford and Okemo breaches to know for sure whether the PCI rules need to be tweaked. Russo vowed that if additional controls are necessary, changes will be made promptly by the council, an independent group that the credit card companies set up in 2006 to manage the standard.

But Russo contended that if a company implemented all of the existing PCI controls, it wouldn't be possible for attackers to get at data while it's being transmitted internally.

"Just because [Hannaford] raised their hand and said they were compliant doesn't necessarily mean they were compliant," Russo said. He added that all of the known data breaches involving companies covered by the PCI rules have happened because the merchants failed to fully comply with the security requirements.

Encrypting payment card data before it even reaches point-of-sale systems is one way to minimize the risk of data-in-transit thefts, Litan said. But tools that could enable companies to do that are just emerging from vendors such as VeriFone Inc., she added. And at this early stage, installing the tools may require a heavy investment of time and effort on the part of users.

■ In the wake of the breaches at Hannaford and Okemo, Airline Reporting Corp. is reviewing its networks to make sure they aren't vulnerable to data-in-transit thefts, says Deven Bhatt, ARC's director of corporate security.

A more straightforward approach would be to better monitor corporate networks for the telltale signs of system intrusions, said Ken Pappas, a security strategist at Top Layer Networks Inc., which sells intrusion-prevention systems. For example, looking at where data traffic is headed could give security managers a clear indication of whether transmissions are legitimate.

The techniques used to pull off data-in-transit heists really aren't all that new. Typically, perpetrators first gain access to a targeted network by taking advantage of a vulnerability that has yet to be detected or patched. Once the attackers get a foothold, they can widely deploy malware that can sniff the network for traffic they're interested in, such as credit card data.

The malware can also be programmed to queue the stolen data and send it in batches to an outside destination, as was the case with the Hannaford intrusion.

Eddie Schwartz, chief security officer at NetWitness Corp., a vendor of network monitoring tools, said that over the past two years, overseas "carder gangs" that buy and sell stolen payment card numbers have been using data-sniffing tools in an effort to intercept information while it's being transmitted across networks.

"People are finally waking up and focusing on it," Schwartz said. He attributed the newfound interest to the attention generated by the breach at Hannaford, which has replaced all of its store servers as part of an attempt to rid its network of the malware installed there.

The data thefts can be hard to detect because often the stolen information is spirited out of a company via open network ports — such as Port 80, which is used for online connections and serving up Web pages, or Port 443, which can be used to send secure communications over the Web.

Schwartz said that many companies don't even monitor those ports, assuming instead that all of the data traffic going out through them is legitimate.

Network managers should be watching the ports "for nonstandard traffic," he added. "If traffic is destined for Romania, and it's [using] Port 443, and it's not SSL traffic, that's a red flag — and you should see it in minutes, not months."

Based on what's known about the Hannaford and Okemo breaches, it isn't clear whether they really do point to a new method of attack, said Deven Bhatt, director of corporate security at Airline Reporting Corp. in Arlington, Va. But he added that ARC, which provides ticket distribution and financial settlement services to more than 150 airlines and rail carriers, is reviewing its networks to make sure they aren't vulnerable to data-in-transit thefts.

ARC's review was prompted by Okemo's disclosure that its systems had been breached in a Hannaford-like fashion and by the reports that other companies may have been similarly attacked. Bhatt noted that ARC is fully compliant with the PCI requirements.

But Hannaford has made the same claim and yet was the victim of a data breach.

Chris Andrew, vice president of security technology at software vendor Lumension Security Inc., said the grocer's network obviously wasn't locked down tight, as evidenced by the fact that the malware was able to send the stolen data overseas.

"Clearly," he added, "there was a pathway back out of the network that Hannaford should have closed." ■

IT Keeps Battling to Maintain Control of Technology

Gains are forfeited as business units demand to make purchases on their own.

By Patrick Thibodeau

LAS VEGAS

COUNTRIES MAY have clear borders, but IT organizations do not. IT managers and analysts at Gartner Inc.'s Symposium/ITxpo here last week said that a growing number of IT units are encountering new resistance in the never-ending battle for control over corporate technology.

In recent years, IT departments have expanded their powers by overseeing corporate initiatives to consolidate data centers and to implement virtualization and data integration projects.

Those efforts allowed IT to regain much of the authority that had been hijacked by business units starting 20-plus years ago with the dawn of the PC revolution.

Today, IT managers face new battles over who chooses the brand of cell phones and PDAs employees use, which specialized manufacturing systems departments can use and which high-performance computing systems researchers can run.

During a forum at the conference, Gartner analyst Colleen Young argued that IT managers must retain strong centralized control of corporate technology and services. She contended that neither research and development organizations nor some business units have the expertise to make technology purchasing decisions on their own.

"It will become very clear very, very quickly that [researchers] lack managerial expertise," said Young. That lack of expertise could force businesses to accept poor deals and adopt inadequate technologies, she added.

Nonetheless, Kristine Blanz, who manages IT operations for an engineering research group at a manufacturer she asked not be named, fears that a centralized process could hurt individual departments.

Blanz said that her company uses a decentralized decision-making process but is reconsidering that approach. She isn't part of a corporate IT organization, she noted.

"If we get wrapped up in corporate IT, the needs of engineering get missed," Blanz said. "What a marketing person needs is not what engineering needs." Centralized decisions could impair "the ability of engineers to innovate," she added.

Kristian Steenstrup, another Gartner analyst, contended that no matter what the policy, IT organizations will always have a difficult time trying to manage some technologies, such as hosted software and consumer devices brought into the enterprise. "There is a lot of technology in your organization that is outside of your control," he said.

■ **IT managers face new battles over who chooses everything from cell phones to high-performance computing systems.**

Allen Benson, an IT manager at a retailer that he asked not be named, said his company recently moved control of its cell phones and mobile devices from the purchasing department back to the IT department.

Previously, he said, employees could "buy everything and anything" they wanted when it came to PDAs and cell phones. That policy led users to request that the IT operation provide e-mail access on a variety of mobile platforms, including many that the company didn't support.

Benson said that IT's decisions regarding what should be under its control are based on whether a particular technology uses the corporate network.

On the other hand, the IT unit will, for example, allow the engineering organization to use advanced technologies that require no internal development and are dependent on the vendor for support. "We really don't want to grab them unless we have to," Benson said.

Centralized control is vital in some industries because of regulatory issues.

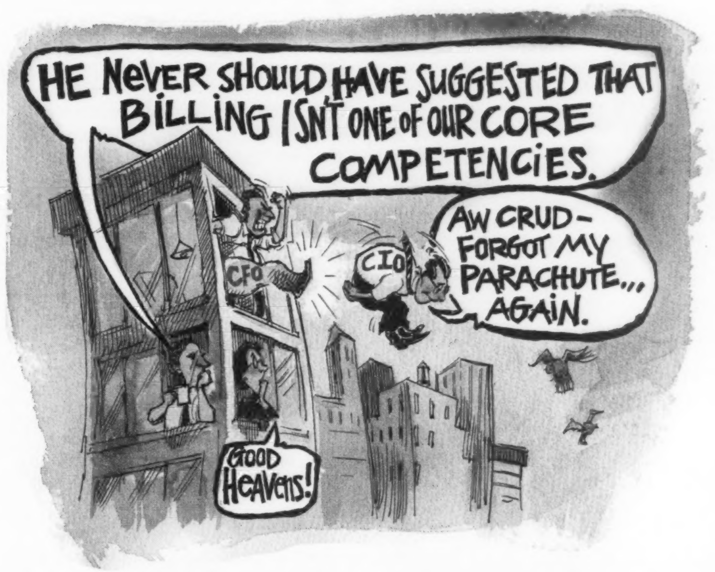
For example, gaming companies are so heavily regulated that any technology that affects guests or cash flow must be certified.

Consequently, Las Vegas-based MGM Mirage can't allow its various entities, which include the Bellagio, MGM Grand and Mandalay Bay hotels, to head off in their own technology directions, said CIO and Senior Vice President Tom Peck.

"We want to encourage properties . . . to be autonomous and come up with ideas," Peck noted, "but we're very centralized from a technology perspective." ■

On the Mark

HOT TRENDS ■ NEW PRODUCT NEWS ■ INDUSTRY BUZZ BY MARK HALL


HE NEVER SHOULD HAVE SUGGESTED THAT BILLING ISN'T ONE OF OUR CORE COMPETENCIES.
AW CRUD - FORGOT MY PARACHUTE... AGAIN.
CFO
CIO
GOOD HEAVENS!

MATTHEW FAULKNER

SaaS Slips Past Last Barrier

CIOs ARE loath to give up direct control of the systems that chief financial officers watch like a hawk. Billing and general ledger software come to mind as programs you'd think would never be candidates for software as a service (SaaS). But that will change. In fact, says Ed Sullivan (no, not that Ed Sullivan), it already has.

Aria Systems LLC in Media, Pa., handles all aspects of recurring billing operations, including service activation and deactivation, usage tracking, and reporting, says CEO Sullivan. All the information can be customized and fed directly into a general ledger. What's more, Aria has been blessed by third parties as being compliant with the Payment Card Industry Data Security Standard, or PCI for short. Aria's Linux-based servers are located in a SunGard SAS 70-audited data center with disaster recovery capabilities. Sullivan has his fingers crossed that by the end of Q2, his application environment will get SAS 70 certification specifically for financial systems.

SaaS for CFOs? Not a pipe dream, claims Sullivan.

Currently, Aria bills more than a million consumers and businesses each month and handles over a billion transactions per day. Maybe the last barrier for SaaS has been breached. Pricing starts at 10 cents per invoice.

Morph SaaS Into DaaS

"Desktops as a service" may be the next catchy buzzphrase if a new virtualization technology from MokaFive Inc. works as advertised. Bill Demas, CEO of the Redwood City, Calif.-based start-up, says the MokaFive service lets you store your company's desktop images — operating system, applications and data — as a tenant "in the cloud."

When a user connects, the service immediately starts streaming the virtual desktop image to his machine. Demas says IT can create, deploy, manage and monitor all the virtual desktops centrally through the MokaFive service.

According to John Whaley, principal engineer, the company's compression tools can fit a package containing Windows, Office 2007 and data into about 1GB, streaming the bits fast enough so users can start working quickly. He says the image can also be stored on a USB drive and booted from there on any x86-class PC. Desktop images on USB drives will be updated as needed when the PC goes online.

100MB
The compressed size of Windows XP via MokaFive, the company says.

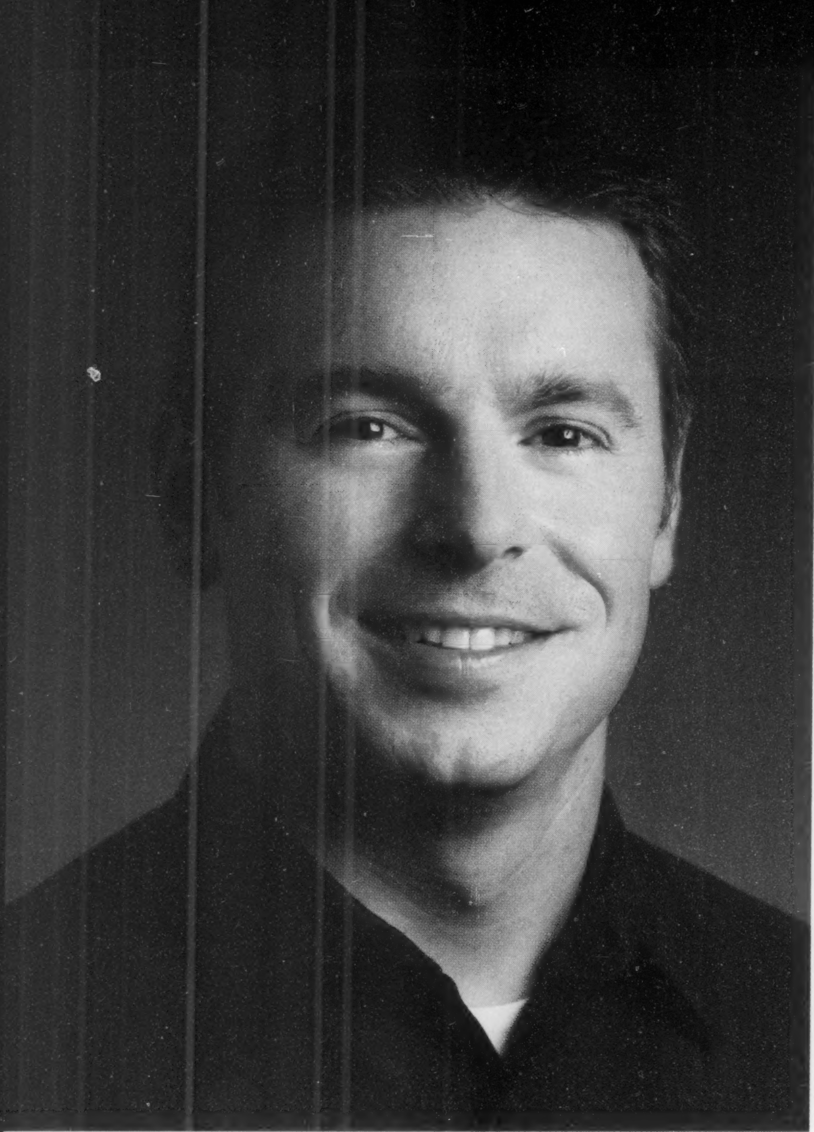
MokaFive supports Windows, Mac OS X and the company's own version of Linux. Pricing will be set when it becomes generally available later in Q2.

A Cure for Boring IT Applications

One reason enterprise applications fail is that they are, well, boring. And Anthony Franco, president of EffectiveUI Inc. in Denver, says the state-of-the-art tools that help developers write apps that appeal to users aren't just about generating a lot of whiz-bang special effects. Rather, they address hard-nosed ROI needs. For example, he says, rich Internet applications (RIA) written using Adobe Flex can run in the Flash player, which makes them cross-platform automatically. Plus, they can run using Adobe's AIR, so a user doesn't have to be connected to a server to get work done. There is one problem, he admits: There's a dearth of Flex developers today. And Microsoft Corp.'s Silverlight remains in beta, so there are even fewer of those. But Franco has 77 RIA experts ready to code. For a price, of course. ■

Franco: Spiff up your corporate apps with AIR and Flex.

COMPUTERWORLD.COM
MORE BUZZ
Discover and discuss more industry action at the On the Mark blog:
computerworld.com/blogs/hall



THE GRILL

Matthew Glotzbach

Google's **enterprise product guru** talks about the **logic of cloud computing,** the emergence of **corporate social networking** and the advent of **true utility computing.**

Google's enterprise guy gets it that corporate users need to become more comfortable with "cloud computing" — software services delivered through the Internet — before it will really take off. But he thinks logic is on his side.

Dossier

Name: Matthew Glotzbach

Title: Director of product management for Google Enterprise

Organization: Google Inc.

Location: Mountain View, Calif.

Pet peeve: "What are people thinking when they get on a full flight and recline their seat into my laptop computer?"

Philosophy: "Extremes are bad (with the exception of triathlons, flying, and driving a Porsche, of course)."

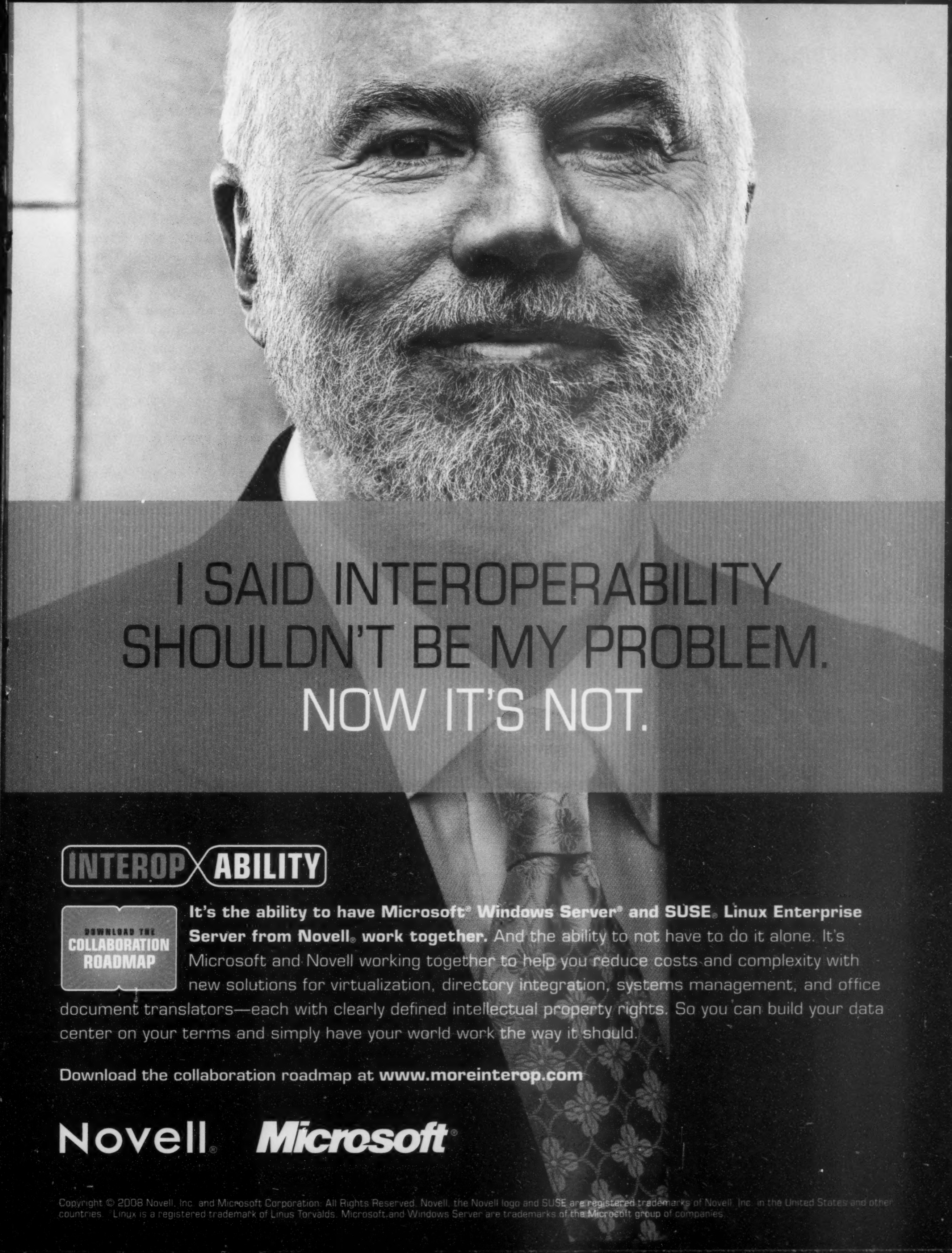
Technology that really fascinates him: "I believe the leading companies and countries in the next decades will be those that figure out how to be more green, more efficient and more entrepreneurial about selling or exporting environmental technologies."

What's so good about cloud computing? Cloud-based applications are just built differently. They're not thought of as "versions"; there's a constant stream of updates. For a large enterprise, from an IT perspective, it's even less about the cost than it is the hassle. It's so difficult to upgrade to the latest version of "X." You may have customized such that upgrading to the new version is nearly impossible. There are things you can do in a cloud model that you can't do in the traditional software space. On the e-mail front, we give 25GB of storage to our business users. That's just not something you can do with a Lotus Notes or Microsoft Exchange system.

How else can cloud computing overstep the bounds of traditional software? One of the areas of research at Google is automated machine translation. What you need to do in real time for automated machine translation is to call up large amounts of compute power, which we have, and large amounts of data, which we have. Imagine if you have a system that can do real-time, on-the-fly translation of things like e-mail documents and IM chats. That's actually a feature [of Google Apps] you can see on the horizon. If you take a traditional or PC or client/server type [application], it's difficult to see how you would ever achieve that.

After one year, has Google Apps met the

Continued on page 22


I SAID INTEROPERABILITY
SHOULDN'T BE MY PROBLEM.
NOW IT'S NOT.
INTEROP ABILITY
DOWNLOAD THE COLLABORATION ROADMAP

It's the ability to have Microsoft® Windows Server® and SUSE® Linux Enterprise Server from Novell® work together. And the ability to not have to do it alone. It's Microsoft and Novell working together to help you reduce costs and complexity with new solutions for virtualization, directory integration, systems management, and office document translators—each with clearly defined intellectual property rights. So you can build your data center on your terms and simply have your world work the way it should.

Download the collaboration roadmap at **www.moreinterop.com**

Novell® Microsoft®

Copyright © 2008 Novell, Inc. and Microsoft Corporation. All Rights Reserved. Novell, the Novell logo and SUSE are registered trademarks of Novell, Inc. in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Microsoft and Windows Server are trademarks of the Microsoft group of companies.

> **“In a rational discussion, it’s pretty easy to believe that our systems are going to be as secure – or, in most cases, more secure – than your average enterprise.**

Continued from page 20

company’s expectations? We now have over 500,000 organizations using Google Apps — from SMBs all way up to large enterprises. The current [enterprise application] systems that people run are so expensive and complex. Cost is a major factor, but also the convenience and the power of the applications is really allowing larger enterprises to take a closer look.

Are enterprises ready for software as a service? We have hundreds of millions of users who trust us with their data, whether it be search history or Gmail accounts or credit card information. We move around, process and store data. In a rational discussion, it’s pretty easy to believe that our systems for doing so are going to be as secure — or, in most cases, more secure — than your average enterprise. I think it’s really an emotional argument.

We’re [also] quickly dispelling this myth that cloud-based or services-based applications are somehow for the lightweight user rather than the power user. Because these apps are connected up in the cloud, they facilitate collaboration and sharing that is nearly impossible for traditional apps.

How will you handle lofty enterprise expectations of service delivery? Our group’s job is to learn from the consumer space and apply it to the enterprise. We try to drive that ease of use and simplicity. Where the enterprise dimension comes into play is around administration controls. It’s making our applications organizationally aware. We can make sharing [within] your company very easy and straightforward. We can put protections that ensure you don’t share things outside. There are APIs to integrate with directory systems. Those types of things are important to enterprises.

How deep can Web 2.0 and social networking content dive into enterprises? I think social networking is really going to find its home in the enterprise. That’s not to disparage Facebook or MySpace or our own [Orkut] social network initiative, but when you think about work and business, it’s all about your network. It’s about who you know and who you’re connected to. I think the existence of a social network and the leveraging of that network is really going to be key as these [hosted] applications continue to evolve. One of the challenges of content management has been exactly that: trying to manage knowledge. It’s almost an untenable task because the knowledge lives with people. The knowledge is all about connections people have with each other. As we look forward to cloud-based applications, you can do these powerful things to understand what those networks look like and how to leverage those for the good of the user.

What is Google doing in that area? The first very simple incarnation of social networks for us is embedding “presence” in more and more places, like calendars, spreadsheets, applications themselves. The cloud facilitates that connected capability. As you move out of a disconnected world into a cloud-based world, we can build our apps from the ground up to be inherently social or inherently collaborative.

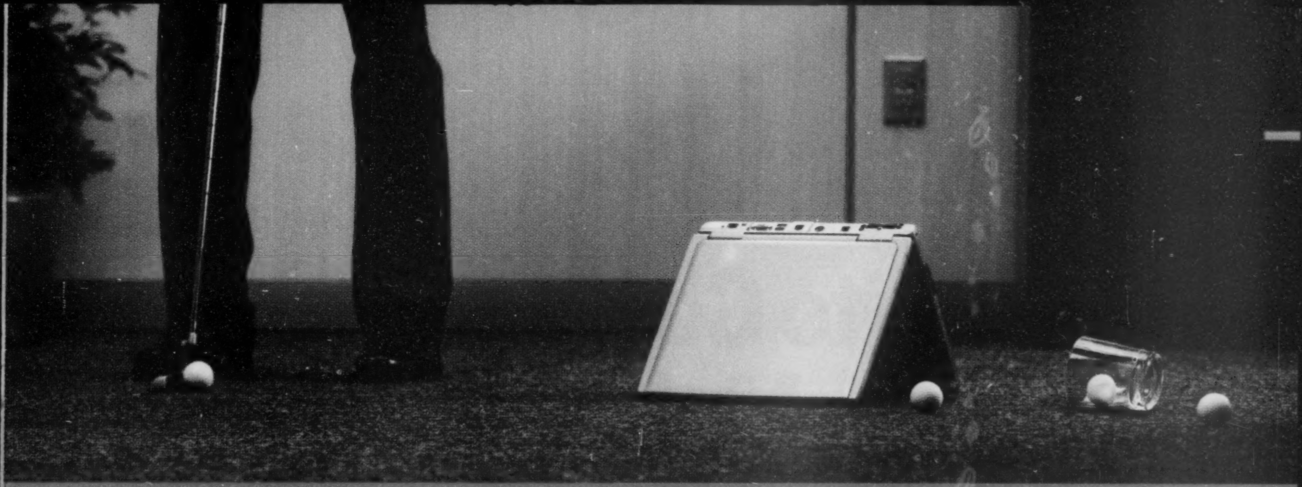
What are some technology areas you may pursue for Google Apps? Video is one of the apps we get asked about all the time, with the popularity of YouTube. Now that video creation and capture is ubiquitous, there are hundreds of uses of video. Videoconferencing has been used forever, but it is extremely expensive. That’s an area that could be interesting. The sky is the limit.

Microsoft has put Google Apps directly in its cross hairs. Are you concerned? I don’t wake up every day thinking about how am I going to beat Microsoft. I think the reason Google is where it is today is [that we] focus on the user, and everything else will take care of itself.

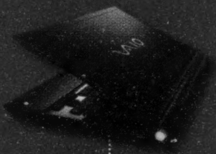
Why is Google better suited to host business apps than Microsoft et al.? We had no legacy. We weren’t trying to take Exchange and host it. That’s probably one of the biggest challenges [for] traditional vendors. They’ve got 30 years of a traditional way of doing things, and it’s very hard to step outside yourself and start from scratch.

What is the future of SaaS? I think we’re going to move more toward a true utility model. Yeah, there may be some connection charge you pay every month to keep the lights on, but you only pay for what you use. And I think software-as-a-service cloud computing applications give us that capability. I see no reason why you should even pay for users; you should really pay for active users. I can see us moving more in that direction.

— Interview by **Brian Fonseca**



Your old notebook can still be put to use.
A new one from CDW can be put to work.



Sony® VAIO® TZ295

- Intel® Centrino® Duo Processor Technology
  - -Intel® Core™ 2 Duo Processor U7700 (1.33GHz)
  - -Intel® Wireless WiFi Link 4965AGN
- Memory: 2GB
- 64GB solid state hard drive
- DVD±RW drive
- 11.1" WXGA display with XBRITE™ technology
- Windows Vista® Business Edition

VAIO PROFESSIONAL

$3499.99
CDW 1392616

Samsung SyncMaster™ 943BX

- 19" analog/digital LCD with dynamic contrast ratio of 8000:1
- Panel brightness of 300 cd/m² and 5ms response time
- Three-year limited parts, labor and backlight warranty

$259.99 CDW 1382353

SAMSUNG

Kensington® sd200v Notebook Docking Station with Video

- One VGA port (supports 1280 x 1024 pixels), five USB 2.0 ports, microphone in and stereo out ports
- Plug-and-play functionality
- Front LEDs show connectivity status

$115.99 CDW 1303339

Kensington

We're there with the technology solutions you need.

Sure, outdated technology can serve your needs. But unfortunately, not your work needs. When you upgrade to new technology from CDW, you'll be more productive than ever. If you need to go mobile, you can with countless wireless options. Need to upgrade to a new operating system? No problem. Of course, we also offer a personal account manager who knows the needs of your business, as well as a host of configuration services. Bottom line – we'll make sure you get what you need, when you need it. So call CDW today and work smarter, not harder.

CDW.com | 800.399.4CDW

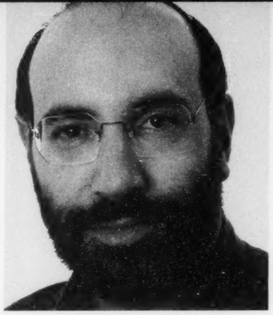
CDW

The Right Technology. Right Away.®

Offer subject to CDW's standard terms and conditions of sale, available at CDW.com. ©2008 CDW Corporation

■ OPINION

Michael Gartenberg



An XP Lite Could Really Go Mobile

I'VE BEEN working with one of the coolest ultraportable Windows XP machines I have ever used. It's a shame that most people will never be able to experience it.

The reason they won't is that, out of the box, the Eee PC isn't a Windows XP machine. It can become one, but it's not an easy task. However, after seeing how great the Eee PC can be after its conversion to XP, I see a big opportunity for Microsoft.

First, though, let me tell you about the Eee PC. It's a fairly limited device from Asustek Computer that retails for only $399 with 512MB of RAM and a lowly 4GB of storage. Out of the box, it has a full Linux environment based on Xandros. That offers a lot of functionality. For example, reverting everything to a working state is a five-minute operation.

But that didn't cut it for me. I want Microsoft Office, PopCap games and a Slingbox client. Thankfully, Asus provides a disk with all the Windows XP drivers you need to get the system running.

I had an XP SP2 install disk, but XP doesn't comfortably fit into the constraints of the Eee PC. Fortunately, a free tool called nLite came to the rescue. NLite lets you custom-install XP with a much smaller footprint.

It's not something for the faint of heart. It took me a lot of trial and error to build a version of XP with an installed footprint of just under 500MB. (The install itself was clean and easy, though.) Next, I installed the Asus drivers and a reduced version of Office 2003, along with a few games. Finally, with a driver for a USB 3G modem and a suite of portable applications, I was all set. And I still had more than half of the 4GB of space on the Eee PC available.

■ **I see a big opportunity for Microsoft here.**

What I have is a tiny, easy-to-carry XP machine that weighs a mere 2 lb. and has everything I need when I'm on the road — and nothing more. The machine boots in less than 20 seconds and shuts down in 10 (no need to hibernate or suspend). In short, it's a cheap yet powerful mobile device that has full PC functionality.

So, what's missing? Well, it could never be my primary machine, although it could serve that purpose just fine for a student if you added a cheap monitor and a USB keyboard for use in a dorm. It's not a media powerhouse, although you can watch movies and listen to music off of a USB card or stick. And it's certainly not a hardcore gaming box.

The problem isn't with what I ended up with, but with what it took to get there. NLite isn't something most users should mess around with, and configuring stuff for portable use isn't something most users will know how or want to do.

But that's simple to fix, if Microsoft wanted to take advantage of the opportunity that the Eee PC and other ultraportables represent. It could make a version of XP optimized for small systems, with a version of Office to match. It's a wonder it hasn't done just that. XP runs everything out there and could even be "skinned" to look like a Vista family member.

The fact is, Vista is just not designed to work well on the vast majority of ultraportable computers, and XP flies in comparison. Instead of taking XP to end of life, Microsoft needs to consider XP as a core mobile platform going forward while keeping Windows Mobile reserved for phone-based devices that are pocketable or smaller. ■

Michael Gartenberg *is vice president and research director for the personal technology and access and custom research groups at JupiterResearch in New York. Contact him at mgartenberg@optonline.net. His weblog and RSS feed are at http://*weblogs.jupiterresearch.com/analysts/gartenberg.

GO BIGFIX OR GO BLIND

SYSTEMS MANAGEMENT IN A VERY DANGEROUS WORLD

BIGFIX actually lets you see. We offer the IT industry's only converged security and operations platform that enables real-time visibility and control of globally distributed desktop, mobile and server infrastructures. Are you using LANDesk, McAfee, Microsoft or Symantec? Relax. You won't have to unplug a thing. We just give you—here's a novel idea—eyes.

For IT pros who want to instantly turn on the lights, call 510-652-6700 x116 or visit www.bigfix.com/geteyes. We'll give you unprecedented visibility. At your site. Any time. And we're betting you won't let us pull the plug after our FREE 30-day tour de force. Because you wouldn't willingly stumble around in the dark, waiting for nocturnal predators.

Visibility Factors	BIGFIX	LANDesk	McAfee	Microsoft	Symantec
Pervasive Asset Discovery	Yes	Blind	Blind	Blind	Blind
Mobile Computer Management/Security	Yes	Blind	Blind	Blind	What's that?
Task Verification Speed	Real Time	Weeks	Weeks	Forever	Weeks
All Popular Endpoint OSs Supported	Yes	Blind	Blind	Huh?	Blind
Number of Administrators Required	1	Dozens	Dozens	Dozens	Dozens
Number of Servers Needed	1	Acres	Acres	Acres	Acres
Number of Agents/Consoles/Toolsets	1	Lots	Lots	Lots	Lots
Time to Implement	1 Day	Months	Months	Months	Months
Total Cost of Ownership	Lowest	Your Job	YourMarriage	Your Sanity	Your Career

BIGFIX®
We mean business

©2007 BIGFIX. BIGFIX and its logo are registered trademarks of BIGFIX, Inc. All other trademarks are sincerely and respectfully acknowledged. TRBA

Whodunit?

Was it the receptionist, the salesman or the building manager who gave away company secrets? Here's how to find and stop the leaks.

By Jennifer McAdams

TRUSTING AN employee with access to mission-critical or sensitive systems is a risky but unavoidable gamble. Let's face it: People are wild cards. In fact, let's take the gambling analogy a step further. Just as casinos thwart cheaters at every table or station on their floors, so, too, can IT officials thwart breaches by customizing security plans for individual employees in every zone of their companies.

In fact, casino practices can be translated to the corporate IT world to create at a common-sense list of do's and don'ts for redoubling security based on who does what job. The lessons we learn from craps pits and blackjack tables reveal that it's never wise to entrust your business's most valuable or vulnerable assets to a single employee. Instead, compartmentalize access whenever possible, and never hesitate to look over employees' shoulders.

Above all, follow the golden rule of a casino: Gauge your level of risk and develop airtight audit trails, urges Bruce Schneier, a security expert in Mountain View, Calif., who has written several books on computer and network security, including *Applied Cryptography* (Wiley, 1996). Schneier often uses the casino metaphor to drive home important points surrounding individualized security. "If you look at a casino floor, you will notice immediately that people are watching people," he says. "That's because a lot of cash is moving, and it's moving very quickly."

Just as edgy casino managers constantly size up everyone on the floor as potential security threats, so must corporate IT security leaders size up every employee. "People are the weak-

est link in security. They always have been, and you will never change that," Schneier says. "But the reality is that you've got to deal with people, and people are going to make mistakes."

Security isn't the responsibility of a single security manager or even a security department. Just as quality was understood in the 1980s to be the responsibility of everyone in an organization, so, too, is security everyone's responsibility (see "Security Team," page 44). Each person in the organization creates, works with, transports and stores valuable information and physical assets. And each employee has a responsibility to safeguard those assets. Unfortunately, too often employees aren't educated by the organization as to what their duties are and how they can effectively manage risk while still getting their jobs done.

And the idea that an organization must guard against nefarious insider activity isn't new, either. "Most effective security programs address the people element, and any job function with access to an organization's valuable resources or assets is a risk," explains Kent Anderson, managing director of Network Risk Management LLC in Portland, Ore. Anderson cites a wide range of personnel who pose mighty risks — everyone from security guards to IT workers to higher-level executives with the authority to override security controls.

The people problem continues to grow, since it is now harder to differentiate between internal and external threats. "The difference between an insider and an outsider is no longer clear," says Anderson, who cautions corporations to be aware of the ways that contractors, outsourcers, vendors, partner companies and suppliers could gain access to sensitive corporate data — either by accident or by design.

While spotting risks can be tricky enough, addressing weaknesses is even tougher, says Anderson. For example, security training programs often prove ineffective, and many employees will continually disregard advice and fail to pay heed to the cautionary tales delivered at droning security seminars.

"The average employee view is one-dimensional. These individuals are not looking at security from the standpoint of accountability for the organization. They are looking at the issue only as it affects their level of responsibility," observes Norris Roberts, director of technology for the Jennings, Mo., school district.

A quarterly employee-awareness seminar might provide a check for a compliance-driven security program, but if the employees are left to try to figure out how to apply security controls to their day-to-day job functions, that will probably never happen, says Anderson.

Roberts rattles off a list of security measures employees are likely to ignore. "Strong password practices are not being applied. The sharing of passwords continues. Good e-mail practices are ignored. And overall, inappropriate user rights and privileges remain a huge problem," he says.

"The most common mistake when educating end users about security awareness is that the training is frequently presented in a Draconian fashion, which does nothing to encourage employees to cooperate with the policies being implemented," notes Eddie Zeitler, executive director of International Information Systems Security Certification Consortium Inc., or (ISC)^2, in Palm Harbor, Fla.

"Security awareness doesn't have to be boring," he says, quickly adding that companies must do far more than just jazz up security training efforts. To make employees more invested, IT shops must convince workers that security measures are imposed for the benefit of both employer and employee.

"If employees realize they could lose their jobs over something that could have been prevented by practicing common-sense security measures, they are given extra incentive to play by the rules," Zeitler says.

Playing by the rules is non-negotiable at casinos, where the stakes are high. Corporations that have just as much to lose must constantly communicate the same message. Only then will granting the privilege of access no longer be such a gamble. ■

McAdams *is a freelance writer in Vienna, Va. You can contact her at JMTechWriter@aol.com.*

BRANDON LAUFENBERG

5 Things YOUR HR People SHOULD KNOW

Huge stores of personnel data make this department a target for thieves.

By Mary K. Pratt

HUMAN RESOURCES departments typically have some of the biggest collections of sensitive data in any organization. But even if companies have corporatewide security measures in place, HR staffers are particularly vulnerable to data leaks because of their departments' vast holdings. The nature of the HR job, which requires nearly constant collecting and sharing of data, presents further challenges.

1 KEEP TRACK OF INCONSISTENT LEGAL REQUIREMENTS.

Companies often keep employee information in one global HR system because it's efficient, says Rena Mears, a partner in the security and privacy services unit at Deloitte & Touche LLP. Yet labor and privacy laws vary from country to country, she says. Data that's considered sensitive and must be encrypted in Europe might need to be more readily accessible for employee-employer transactions in the U.S.

>>> IT's response: Assign ownership and responsibility. Companies must bring together stakeholders — HR executives, the chief privacy officer (if there is one), the chief security officer and IT architects — to sort through the complex requirements, develop processes for handling data, and design applications that include appropriate safeguards, such as encryption and restricted access, for each location.

2 DON'T COLLECT UNNEEDED INFORMATION.

The University of Nebraska, like many organizations, once used Social Security numbers to identify employees. But this practice increased the chances for sensitive data to fall into the wrong hands, says Joshua Mauk, the university's information security officer.

>>> IT's response: Pare down the amount of information that is collected. Mauk says the university looked at the information it was gathering and determined where it could forgo the use of Social Security numbers. IT developed a process that now allows HR to assign workers unique numbers known as NUIDs that can be used on forms and records.

3 PROTECT SENSITIVE DATA IN EVERY LOCATION.

Today, personnel data exists not only on paper, but also in electronic files that can reside in multiple locations. What's worse, many of those locations may be orphaned — and left unsecure. "HR people in the field can have a bunch of information which may never make it back to a centralized HR office," Mauk says, "but that information has to be protected as much as the organization's ERP."

>>> IT's response: Seek, monitor and manage all personnel data. Organizations must adopt records retention policies that specify what documents are kept where and by whom. The policies must also say how those documents should be stored and for how long.

The University of Nebraska uses an application that scans files and servers for sensitive data, allowing Mauk to find information residing in unauthorized or unmanaged areas.

4 SECURE YOUR PAPER FILES.

Improper handling of paper files is an ongoing problem, according to a number of security experts. "We still use paper a lot, but we focus so much on technology that we have a tendency to minimize paper," says Howard A. Schmidt, security strategist at International Information Systems Security Certification Consortium Inc., or (ISC)^2, and a former government and corporate security executive.

Moreover, Schmidt says, because data protection often falls under the purview of the IT department, policies addressing the protection of paper files can fall through the cracks.

>>> IT's response: Assign ownership of updated paper management policies. Companies need to implement policies on how to secure paper records and when to dispose of them. They should also provide ongoing training to HR staffers to underscore why those policies are needed and improve compliance reviews to ensure that the policies are followed.

5 SHARE INFORMATION – CAREFULLY.

HR professionals often need to share sensitive and legally protected information with colleagues inside and outside the company. That sharing, however, creates opportunities for data leaks, says Brad Johnson, a vice president at SystemExperts Corp., an IT compliance and network security consulting firm in Sudbury, Mass.

>>> IT's response: Use automated and multilayered protections. Automatic encryption will help safeguard any data that's being electronically transmitted. And Johnson points out that automatic log-outs and session timeouts can help ensure that sensitive information doesn't remain visible on PC monitors when workers step away from their desks. ■

Pratt *is a* Computerworld *contributing writer in Waltham, Mass. Contact her at marykpratt@verizon.net.*

_INFRASTRUCTURE LOG

_DAY 84: Feeling really disconnected. We're not getting the most out of our existing assets. Service and application integration is a nightmare. We've got to stop working on these islands.

_Please rescue me from this lack of connectivity.

_DAY 87: We're saved! With IBM WebSphere solutions we can service-enable and connect our existing assets for mission-critical goals. Now we can reuse existing applications and save money by eliminating redundant systems. We're ready for any SOA integration project.

_Plus, no more jellyfish stings.

WebSphere.

Download the enterprise service bus white paper at:
IBM.COM/**TAKEBACKCONTROL**/CONNECT

IBM, the IBM logo, WebSphere and Take Back Control are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries.
© 2007 IBM Corporation. All rights reserved.

5 Things YOUR Salespeople SHOULD KNOW

Your road warriors could be leaving a trail of customer data behind them. **By Mary K. Pratt**

THE SALES department's performance is measured on revenue, not on data protection. So it's no surprise that salespeople focus on closing deals, not security holes. As a result, they sometimes sacrifice security for convenience. They log onto Wi-Fi hot spots in airports to work on presentations despite the risk of being hacked. They carry reams of information, some of it propriety, on their smart phones. They transfer deal details on USB drives. Although companies have done much to address the challenges of this frequently mobile population, there's still more work to do.

1 BE WARY OF UNSECURED CONNECTIONS.

Salespeople have the tools to phone home from anywhere. Unfortunately, those connections aren't always secure. Even if a salesman is using his laptop at a Wi-Fi hot spot at the airport just to check sports scores, he could be putting a slew of sensitive information at risk.

>>> IT's response: Mandate encryption and a connection to the corporate virtual private network. Peter Evans, director of marketing at IBM Internet Security Systems, says employees should always use a corporate VPN and encryption to ensure that hackers can't get in. Moreover, companies should automate the process for users so they have no excuse for trying to circumvent the rules.

2 GUARD ACCESS TO THE CRM SYSTEM.

Customer relationship management systems give sales departments an efficient way to handle information. But Rena Mears, a partner in the security and privacy services unit at Deloitte & Touche LLP, says it's often too easy for salespeople to access the system to enter, read or forward information. "You can have data proliferating in ways that you can't control," Mears says.

>>> IT's response: Set policies governing access, and back them up with IT controls. Companies must establish who should have access to the CRM system and for what reasons, Mears says. IT should implement access controls, automated encryption and content-monitoring applications.

3 KEEP A CLOSE EYE ON MOBILE DEVICES.

Mobile devices regularly go missing as a result of carelessness or theft. In fact, a 2005 study sponsored by data protection company Pointsec Mobile Technologies (now owned by Check Point Software Technologies Inc.) found that 85,619 mobile phones, 21,460 handhelds or pocket PCs, and 4,425 laptops were left in a Chicago cab company's vehicles in a six-month period.

>>> IT's response: Deploy security applications to company-issued devices. Businesses should require salespeople to use only company-issued mobile devices that are equipped with automatic protections — boot-up and screen passwords, as well as automatic encryption of data, e-mail and hard drives, says Jonathan Gossels, president and CEO of SystemExperts Corp., an IT compliance and network security consultancy in Sudbury, Mass.

4 CUT THE CELL PHONE CHATTER.

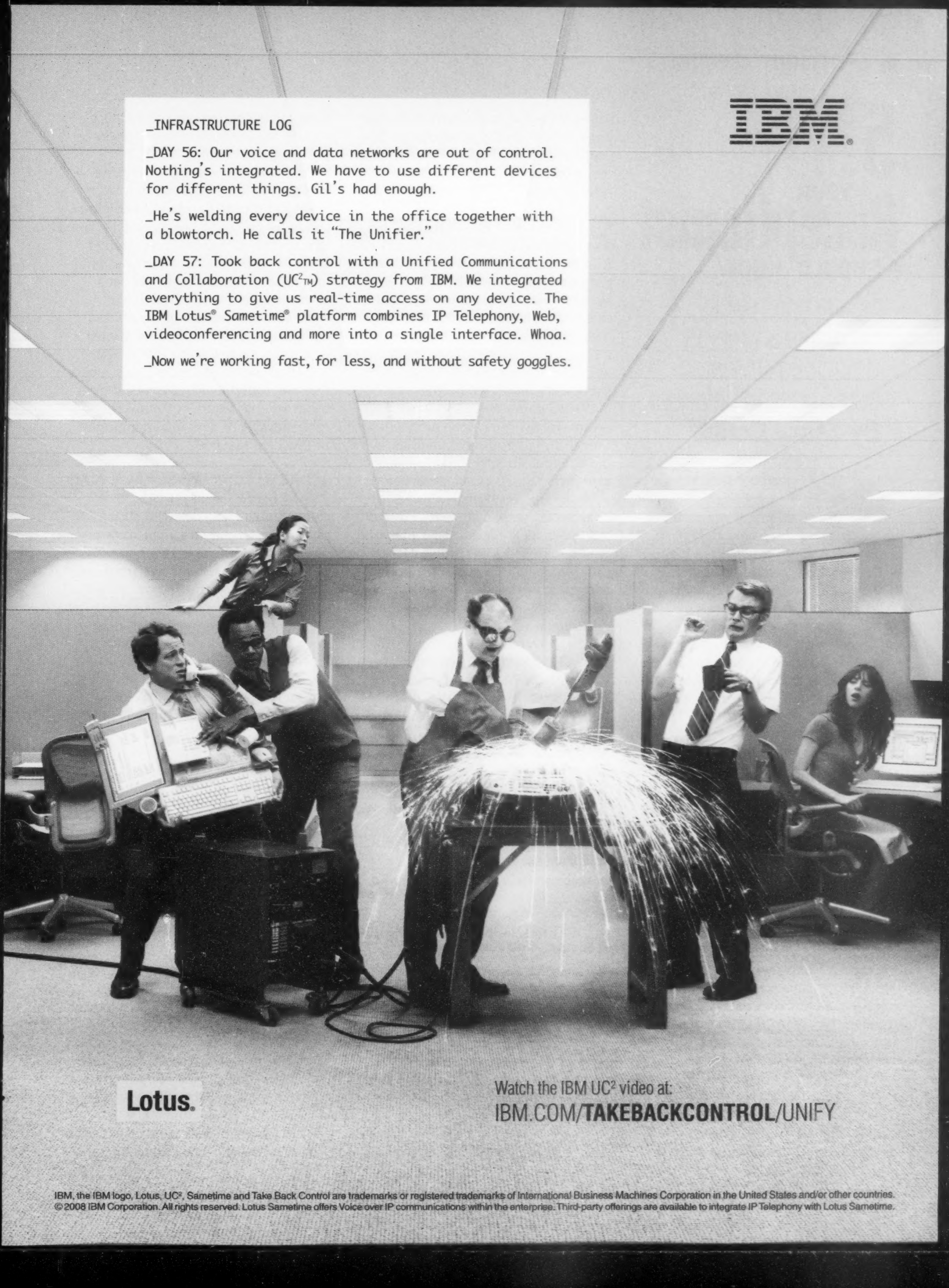
People have a tendency to use their cell phones to carry on public discussions of confidential matters, says Howard A. Schmidt, a security strategist at International Information Systems Security Certification Consortium Inc., or (ISC)^2, which offers the Certified Information Systems Security Professional certification. He remembers once hearing all of the details of a fellow traveler's business call at Dulles International Airport. "Everyone in the cabin could hear him," he says.

>>> IT's response: Provide education. Awareness training is often enough to remind people to watch what they say and when. "We show [video of] people running their mouths really loud and ask, 'Is this you?' " says Schmidt, who has also served as the cybersecurity adviser to the White House and in security roles at eBay Inc. and Microsoft Corp.

5 CURB ACCESS TO ALL THAT INFORMATION.

Not everyone in the sales department has equal responsibilities. Why should they all have equal access to information? Companies often fail to ask that question, says Ed Zeitler, executive director of (ISC)^2.

>>> IT's response: Manage information access and reinforce that effort with technology. Sales managers, security personnel and IT workers should define who needs access to what information. Once that's done, IT should use access controls in databases and applications to ensure that only authorized individuals can get in. Moreover, that team of managers must update access controls when employees' responsibilities change. ■



_INFRASTRUCTURE LOG

_DAY 56: Our voice and data networks are out of control. Nothing's integrated. We have to use different devices for different things. Gil's had enough.

_He's welding every device in the office together with a blowtorch. He calls it "The Unifier."

_DAY 57: Took back control with a Unified Communications and Collaboration (UC^{2}™) strategy from IBM. We integrated everything to give us real-time access on any device. The IBM Lotus® Sametime® platform combines IP Telephony, Web, videoconferencing and more into a single interface. Whoa.

_Now we're working fast, for less, and without safety goggles.

Lotus.

Watch the IBM UC^{2} video at:
IBM.COM/**TAKEBACKCONTROL**/UNIFY

IBM, the IBM logo, Lotus, UC^{2}, Sametime and Take Back Control are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries. © 2008 IBM Corporation. All rights reserved. Lotus Sametime offers Voice over IP communications within the enterprise. Third-party offerings are available to integrate IP Telephony with Lotus Sametime.

5 Things YOUR Receptionist SHOULD KNOW

Scammers, social networks and illegal downloads threaten your front-line defense.

By Stacy Collett

RECEPTIONISTS are at the front line of communication with customers and guests, which often makes them the first targets for hackers and saboteurs looking for company information.

Often young business neophytes, receptionists can be eager to show their competence, and they might inadvertently supply too much information to a persistent caller or visitor. They might also stave off boredom by checking their personal e-mail or surfing the Web. Here's what they need to know.

1 DON'T TRUST STRANGERS.

Social engineering scams — where crooks extract information from victims through interaction and by building trust — is on the rise, according to Bill Nichols, an information security consultant at Control Risks Group Ltd. in Washington. Receptionists represent a prime target because they have access to employees' phone numbers and home addresses and, in some cases, to company systems. The scammer gathers bits of information over time, becomes increasingly credible and eventually gains access or passwords. "That's a real situation that we see all the time," Nichols says.

>>> **IT's response:** A clearly written policy should classify what information shouldn't be distributed. Access to financial or human resources databases, as well as to sensitive customer information, should be restricted. Receptionists should also be trained with real-world scenarios to learn how to respond to information requests.

2 SOCIAL NETWORKING SITES CAN HOLD DANGERS.

Receptionists might kill some time by browsing their Facebook or MySpace accounts, watching an online video or downloading music. But malicious code can now be hidden in video streams, downloaded from YouTube or embedded in songs streamed from social-networking Web sites.

What's more, Web users often have no control over the audio or video they browse. "You can embed these media types directly into Web pages," said David Thiel, a consultant at iSec Partners Inc., an applications security consulting company in San Francisco, in a February webcast. "So for anybody who browses to a Web page, a lot of different media file types are launched automatically as background music or embedded video" without the user clicking on anything.

>>> **IT's response:** Install a filtering proxy. IT departments can block access to social networking sites completely with firewall software. "But if you want to be more liberal and allow [access], use a filtering proxy to check what's coming across and get rid of the known nasty stuff," says Avishai Wool, chief technology officer at Algorithmic Security Inc., a firewall management company in Reston, Va. "You could also include mail filters on incoming and outgoing e-mail to strip out executable attachments. You don't want to be the deliverer of malware, either."

3 PEER-TO-PEER SOFTWARE CREATES LEGAL RISKS.

For many employees, their PCs at work are more powerful than their home computers, and receptionists might want to take advantage of the ample bandwidth to download or share large files using peer-to-peer software like eMule, Kazaa and BitTornado. Problem is, that opens up the organization to potential legal risk.

"A lot of the content is either pirated, illegal, inappropriate or copyrighted," Wool says. "So the organization is opening itself up to legal problems by hosting the content on their servers — even inadvertently."

On the IT side, peer-to-peer products are resource hogs and can easily drain significant chunks of bandwidth meant for company business. The adware they distribute can bombard systems with advertisements and pop-ups, hijack Web browsers and even slow computers to a grinding halt.

>>> **IT's response:** Block access and train employees. IT staffs are almost uniformly against using P2P services, and they take measures to block access to them. Individual employees should be aware that company policies prohibit viewing or downloading pirated or indecent material.

4 KEEP YOUR PERSONAL E-MAIL ACCOUNT PERSONAL.

Receptionists who access their personal Yahoo, Hotmail or Gmail accounts at work open up the network to potential malware attacks. What's more, they may be violating the company's compliance requirements.

At regulated companies, sending company files to a home computer could violate corporate guidelines. "If the file that you sent to yourself goes through [the Web mail provider's] network, then they have a copy of what you sent, and they don't throw it away — so you personally lose control of that information," Wool says.

>>> **IT's response:** Block access to known personal e-mail providers and train employees.

5 BEWARE THE MESSY DESK.

Incoming and outgoing postal mail containing corporate information crosses the receptionist's desk daily. "Clean desk" policies are often not enforced, and a lot of information that can be readily used by scammers may be in plain sight. Even worse, passwords are often left under keyboards or even taped to computer monitors.

>>> **IT's response:** Tighten up paper security. Keep the reception desk clear of visible mail and papers. And have a strong policy that outlines when to shred company documents. ■

Collett *is a* Computerworld *contributing writer. Contact her at Stcollett@aol.com.*

4 Things YOUR Administrative STAFF SHOULD KNOW

Just one step from the executive is a worker who often has high-level data access. **By Stacy Collett**

ADMINISTRATIVE staffers may not have their fingers on the pulse of business-critical operations, but they do get their hands on a lot of sensitive company information.

Executives often grant administrative assistants and record-keepers access to strategic data and correspondence to make their own lives easier. As a result, these well-meaning assistants are often targets of hackers, scammers and even espionage.

1 BEWARE OF 'PRETEXTING.'

Up to 70% of IT breaches are internal in nature, according to Douglas Beaver, vice president, North America, at Asero Worldwide Inc., a Washington-based security consulting firm. In many cases, employees give out information accidentally.

Administrative staffers must guard against pretexting scams, which involve setting up a scenario to persuade a target to release information or perform an action.

"It's typically done over the phone," Beaver explains. "It's not as simple as a lie. The pretexter does some prior research and uses pieces of known information, such as a birth date or Social Security number, to establish legitimacy in the mind of the target." That information can include how to access systems, customer information or any variety of data.

"There's a lot of turnover in these positions, and generally it's a younger workforce," he says. "The inexperienced workforce is more prone to fall prey to pretexters."

>>> IT's response: Beaver advises companies to train staffers on how to properly screen calls. Establish policies on what information they can or can't release, and retrain them with real-world examples on a regular basis.

2 ADMINISTRATIVE STAFFERS CAN BE ESPIONAGE TARGETS.

In 2005, Israeli fraud investigators cracked a major espionage case in which several corporations hired private investigators to secretly install software on administrative staffs' PCs. The machines became infected by a Trojan horse that would steal financial information.

According to investigators, the hacker who created the program used two methods to plant his malicious software in the target computers. One was to send it via e-mail. The other was to send a disk to the target company that purported to contain a business proposal from a familiar firm that would arouse no suspicions. Then, when an employee loaded the disk to view the proposal, the Trojan horse would infect his computer.

>>> IT's response: Make workers aware of the various methods of espionage. "Losing sales projections for next quarter is potentially much more damaging than getting a virus on the network that inconveniences the IT department," says Avishai Wool, chief technology officer at Algorithmic Security Inc., a firewall management company in Reston, Va.

3 DON'T ACCEPT GIFTS FROM STRANGERS.

Most administrative staffers are happy to pick up a few free items at a conference or trade show. But those disks and memory sticks can come loaded with software that could disrupt your systems.

>>> IT's response: Set a policy discouraging employees from bringing these items to work. "If somebody gives you a free CD or DVD," even at a trade show or business conference, "don't plug it into your work computer," Wool says. "Definitely don't plug in USB sticks," because they can contain software that can launch automatically, he adds.

4 IF YOU WANT TO MOVE UP THE CORPORATE LADDER, KEEP YOUR RECORD CLEAN.

When administrative assistants are hired, the position might not call for a criminal or financial background check. But as they move up the corporate ladder, a clean record becomes more important.

Tell staffers that they should expect to be "revetted." They should keep their personal finances and police records spot-free.

"You have an administrative staffer working at a junior level who now has a credit card for booking travel. Or the CEO might have a massive expense account, and they're not going to notice if [the staffer] buys a computer to sell on eBay when paying the bill," says Bill Nichols, a senior consultant and practice leader at Control Risks Group Ltd. in Washington.

>>> IT's response: Run occasional checks. Knowing that an employee hasn't committed a crime or gotten into financial difficulty since his initial hiring will reduce risk. ■

3 Things YOUR Facilities GROUP SHOULD KNOW

These workers literally hold the keys to your company's physical security.

By Julia King

HERE ARE two facts from security experts: First, physical access always trumps technical savvy; and second, facilities and maintenance staffers make soft targets.

That's why Eric Cowperthwaite, chief information security officer at Providence Health & Services in Seattle, recommends developing specific training and awareness programs for building managers, cleaning crews and other facilities workers.

"The key is using multiple delivery tools, including electronic, in-person and paper [presentations]," he says. Providence, for example, distributes trifold brochures, and cards that workers can carry in their wallets. Every month, a half-page security bulletin goes out via e-mail that addresses a new security topic and offers three to five tips on how to recognize a threat and prevent it.

Keep these three things in mind when considering potential threats at your company.

1 DON'T ASSUME ALL IS AS IT SHOULD BE.

If a person is wearing a badge, most employees assume that he is authorized to be there. But crafting a counterfeit badge is well within the talents of your average 10-year-old with a color printer, notes Michael Theis, chief of cyber-counterintelligence at the U.S. National Reconnaissance Office.

>>> IT's response: Security training "should aim to get employees invested in the idea that they need to be curious," Theis says. "If you see someone you don't recognize, ask them who they are."

Darryl Lemecha, CIO at Vertafore Inc., provides the company's security guards and janitorial and building staffs with a list of names and photographs of outside service workers, such as delivery and cleaning people who are authorized to enter the building.

2 BEWARE BIG RISKS IN SMALL PACKAGES.

Incoming letters and packages can easily be tampered with en route, but they are rarely inspected closely upon arriving at a company's mail facility. This can cause big problems, especially for companies like Vertafore, which frequently receives CDs, tapes and other media containing customer data.

>>> IT's response: Vertafore has developed a process of due diligence to make sure that all packages are intact before they're accepted. "We refuse packages that have been damaged in shipping, because customer data may have been lost or tampered with," says Lemecha.

3 NOW'S THE TIME TO CHANGE THE ACCESS CODES.

Four- and five-digit push-button locks on corridor doors, elevators and even data center doors offer another line of defense against intruders. But all too often, the access codes remain the same for years, experts say. That means anyone who has ever worked in that building can still enter areas that should be off-limits to them.

"The building I'm in has a code on the elevator, and the code hasn't changed since we moved in three years ago," says Chris Blake, workstation administrator at The Benchmark Group. "Everyone who has ever been in this building knows the code, but the building owner has been reluctant to let us change it."

>>> IT's response: Have a regular schedule for changing access codes to secured areas. Also, when employees leave a company, their key cards should be deactivated and their badges confiscated and destroyed. ■

---

4 Things YOUR Remote STAFF SHOULD KNOW

Your telecommuters are out there in the ether, along with all your company data.

By Julia King

NO MATTER their job title, business department, industry knowledge, computer savvy and/or exposure to security training, end users are the second-weakest spot in every organization's security fence. They are bested only by one subgroup of employees — remote workers.

Think of the person who works in a satellite or branch office, perhaps with just one or two other employees. Think of the person who works three days a week at corporate headquarters and then travels with his laptop or telecommutes on other days. Think of the countless salespeople working from hotel rooms, airport gate areas, customer sites and Starbucks shops. These are the people who cause security managers to lose the most sleep.

1 BE AWARE THAT ALMOST EVERY DATA DECISION HAS A SECURITY IMPLICATION.

Security awareness training typically occurs on an annual basis, yet remote users make hundreds of security choices every week in the course of their work, says Carol Suchit-Hudson, director of citywide security for the New York municipal government.

For example, should they pop into

the corner coffee shop and hop on its wireless network to answer an urgent e-mail? Or if their flight is delayed, should they use that extra hour to work on that customer spreadsheet?

>>> IT's response: One of the best ways to ensure that remote workers make the right decisions is to offer them more frequent training coupled with periodic security reminders that are tailored to the way they work.

"The appropriate step is to tweak your education program based on the type of user," says Suchit-Hudson. That means using real-life examples and anecdotes. "No one wants to sit through training that isn't applicable to their needs," she says.

2 YOUR CHILDREN AREN'T AFRAID TO DOWNLOAD.

"Mom, can I use your computer to check online for my homework?"

Answering "yes" to this question — as many parents do — can open the gates to security hell, experts say. "Letting kids and others download programs and data of unknown origin onto their machines is one of the biggest worries we have for telecommuters," says Matthew Kesner, chief technology officer at Fenwick & West LLP in Mountain View, Calif.

>>> IT's response: Even the most Draconian of usage policies won't end such incidents altogether. Instead, try appealing to users' self-interest, Kesner advises. If a user has downloaded an unauthorized program or left a wireless connection open after working at home, it will really slow their computer down, he notes. "That's how we message it," he adds. One more tip: Regularly monitor users' hard drives.

3 BE A RESPONSIBLE GADGET GEEK.

BlackBerries, flash drives, mobile phones and handhelds frequently contain critical corporate data, yet most users treat these relatively low-cost devices far more casually than laptops.

>>> IT's response: "Our rule is, if we don't own it, you don't plug it into our network," says Chris Blake, workstation administrator at The Benchmark Group, an architectural and engineering firm in Rogers, Ark.

Another option is to instead have users upload and download data from the server and to encrypt all data transmissions, he says.

4 DON'T FORGET IT – SHRED IT.

Paper may seem quaint in our increasingly digital world. Yet, it's actually quite dangerous if tossed around carelessly, says Darryl Lemecha, CIO at Vertafore Inc., an insurance software and services company in Bothell, Wash. "Dumpster diving remains a common way for thieves to get information," he says. "People have become quite accustomed to shredding at work, but there are still individuals who work from home who are without a shredder."

>>> IT's response: Shredders for all. And they should be cross-cut shredders, so thieves can't piece back together documents that have been torn in only one direction. ■

Scanning speed that blows away the competition. The dependable i780 scans at up to 130 ppm—even when scanning at 300 dpi resolution in color, grayscale or black-and-white, in dual stream mode, with all advanced features enabled. Gain gale-force productivity.

Kodak i780 Scanner

Kodak

©Kodak, 2008. Kodak is a trademark.

Visit kodak.com/go/galeforce

How to Spot a Spy

Con artists make it their job to extract sensitive corporate intelligence from unsuspecting employees. Here's how to stop them. **By Mary Brandel**

BRANDON LAUFENBERG

CORPORATIONS are woefully unprepared to counter attempts at corporate espionage, say experts who perform vulnerability assessments designed to uncover security weaknesses. U.S. corporations lose as much as $300 billion a year to hacking, cracking, physical security breaches and other criminal activity, according to Ira Winkler, author of *Spies Among Us* (Wiley, 2005) and president of the Internet Security Advisors Group, which performs espionage simulations and provides other services.

Although espionage is usually associated with high-tech approaches involving wireless security breaches and zombified PCs, low-tech tactics such as walking into a building are common, says Johnny Long, a security researcher at Computer Sciences Corp. and author of *No-Tech Hacking* (Syngress, 2008).

"To me, computers are irrelevant," Winkler says. "It's about what data do I want, what form does it take, and how can I steal it?"

Any company can be a target, says Peter Wood, chief of operations at First Base Technologies, a U.K.-based consultancy that performs ethical hacking services. Spies are interested in anything from financial data to intellectual property and customer data. They might steal information for blackmail purposes, but "the most common motive for physical intrusion is industrial espionage," he says.

Here are several of the most common ploys and the countermeasures you can put into place to spot — and possibly even stop — the work of a spy.

TAILGATING

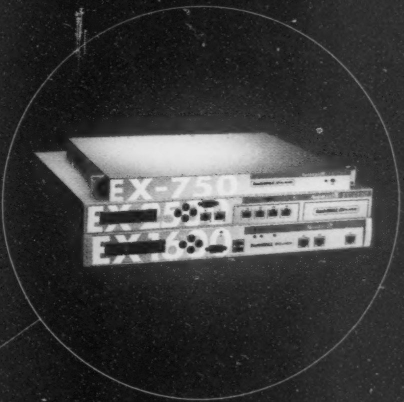
One of the most disturbingly successful ways for outsiders to infiltrate an organization is also the least high-tech: following an authorized employee through the front door. "In 90% of the companies I've worked with, it's so simple to get in, it's pathetic," Winkler says. To blend in, the spy might hold a cup of coffee or a sandwich, dress in a suit minus the jacket or even wear a counterfeit badge.

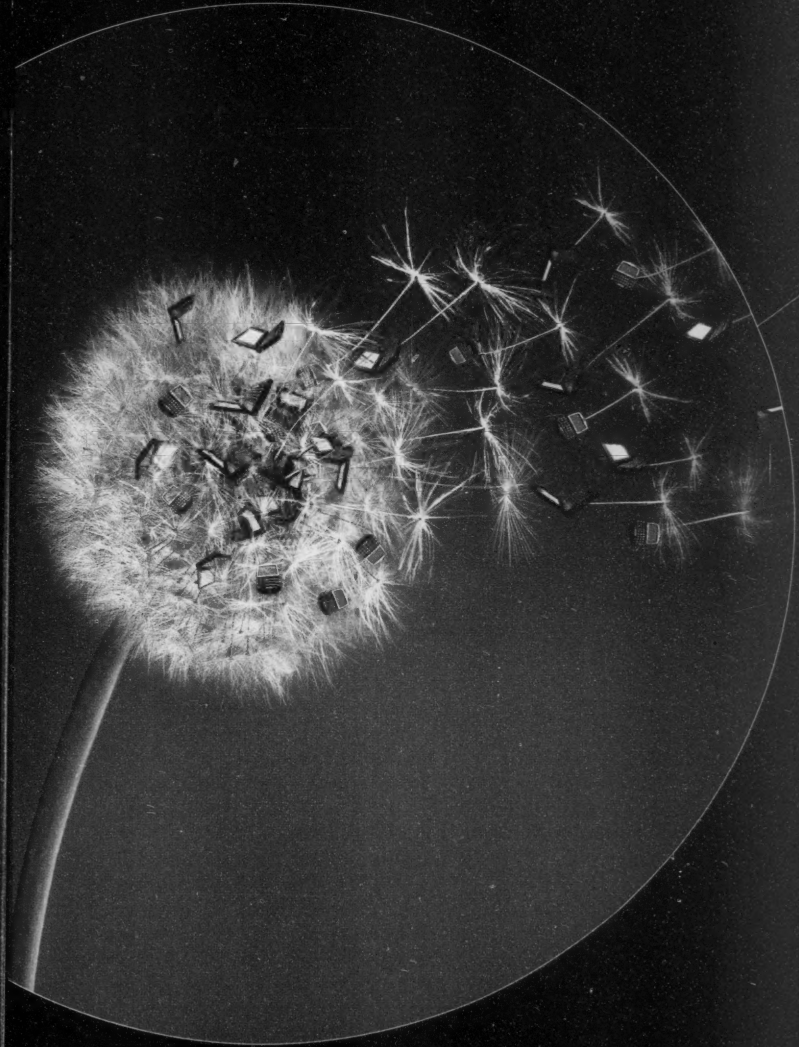
Antismoking regulations have also made it simple to sneak into buildings through the back door, where smokers tend to huddle, Wood adds. And Long

Continued on page 38

SonicWALL E-CLASS

WISHING FOR SECURE REMOTE ACCESS CONTROL?
GRANTED!





SO MUCH FOR THE STATUS QUO.

Existing enterprise-class remote access and SSL VPN solutions fall short—especially when it comes to granular endpoint control, the types of devices they can accommodate, or the ease of administering security policies. Even worse, these solutions can be susceptible to vulnerable connections—actually serving as conduits for malicious code or non-compliance. The SonicWALL® Aventail E-Class SSL VPN solution establishes, manages, and enforces granular application access policies for external and internal users using all types of endpoints including laptops, smartphones, or other devices. The E-Class SSL VPN EX-2500, EX-1600 and EX-750 provide comprehensive interrogation and remediation, establishing trust before access is granted. The E-Class SSL VPN solution is compatible across a broad range of platforms and OS types. When a SonicWALL Network Security Appliance is used with an E-Class SSL VPN, the combined functionality uses deep packet inspection along with granular access controls to decontaminate traffic and to allow authorized application access from any remote device. This combined solution blocks malicious code or any type of unauthorized access. Learn more about SonicWALL's E-Class SSL VPN solutions at **www.sonicwall.com/dandelion** or call **1.888.557.6642**.

SECURE
REMOTE ACCESS

SONICWALL
PROTECTION AT THE SPEED OF BUSINESS

© 2008 SonicWALL, Inc. SonicWALL, the SonicWALL logo and Protection at the Speed of Business are registered trademarks of SonicWALL, Inc.

Continued from page 36

claims to have walked right through delivery or loading dock doors.

Once they're inside, spies have lots of ways to access sensitive information. They can pose as IT support personnel, photocopying papers they find on unattended desks or at printers. Or they can just walk into an empty meeting room, plug in a laptop and pull data off the network. In that scenario, a convincing ploy is for spies to work in pairs, with one posing as a consultant and the other as an employee, says Wood, who has used that tactic. If someone enters the room, Wood says he apologizes for the "double-booking" and moves on. "It's just a matter of having the right attitude and being confident," he says.

>>> How to stop them: According to Winkler, you can't just establish policies; you must also enforce the rules that prohibit security guards, receptionists and other workers from letting people into the building if they can't prove that they're employees. Companies also need to set clear procedures for reporting suspicious people. No one wants a vigilante culture, "but if you see someone acting unusually, you should make note of what that person is doing," Winkler says.

POSING AS AN EMPLOYEE

Spies often pretend to be IT support personnel because it enables them to look legitimate while sitting at users' PCs. The tactic involves either looking for vacated offices or blatantly asking employees to leave their desks so the spy can, say, update the antivirus software. In other cases, spies have posed as cleaning staffers, gaining after-hours access.

Winkler says he was once hired to expose a company's security vulnerabilities but was asked to avoid accessing the CEO's system. However, as he was leaving the executive suite, an assistant asked him, "Why didn't you update Mr. So-and-So's computer?" "There I was, sitting at the CEO's desk at a Fortune 50 company," he says. "I tried to avoid seeing anything sensitive, but I had to pretend I was doing something."

>>> How to stop them: Employee awareness goes a long way. "Most organizations don't even remotely invest in staff awareness," Winkler says. "Most people seem to assume if you're in the building, you must be OK, and that's a presumption that criminals rely on. You need to have standards for what is and isn't appropriate and then reinforce that with a mind-set of challenging people who don't adhere to those parameters."

A second line of defense is to use protective tools like screen savers with password controls, and to encrypt data and require strong passwords for employees with liberal access rights, such as IT administrators and C-level executives. "Most networks are poorly protected," Wood says. "We see trivial, stupid passwords in every firm we visit. Often, the password is the same as the account name."

Finally, classify information in terms of how valuable it is and store it accordingly, says Wood. Even by applying encryption and password controls to just the accounts of IT administrators and senior staff members, companies could solve 70% of the problem, he says. "It would make [accessing information] so much more difficult that it would be a major accomplishment," says Wood.

POSING AS A VISITOR

Another way of infiltrating a corporation is by posing as a legitimate visitor, such as a telephone or electrical maintenance person, a burglar-alarm inspector or someone from the fire department checking smoke detectors.

Wood says he creates convincing costumes by purchasing a fluorescent jacket and work boots and downloading iron-on logos from the Internet. "The whole thing can cost $7," he says, which goes to show how useless physical credentials like business cards are today. Some things he has found while walking around buildings posing as a visitor include customer account details, payroll data disks, a voice-mail guide with default passwords, information about spending on advertising, bank statements, a staff directory, and whiteboards covered with notes about corporate strategy.

>>> How to stop them: The identities of outsiders seeking access to the building must be verified with more than ID cards, Wood says. An employee should ask a visitor to identify his employer, and then the employee should verify the information on the Web and follow up with a phone call to the company to ensure that the visitor is legitimate. "It's tedious but necessary," Wood says.

Persistence pays. Once, when Winkler was posing as a person from corporate who needed a tour of a facility, he was interrupted by a manager who asked why he was being shown around. Winkler gave him a West Coast phone number. "It was 8 a.m. on the East Coast, so by the time he could reach anyone, I was out of the state," he says.

PHISHING

As defined by Wikipedia, phishing is a form of social engineering in which spies use a collection of techniques to manipulate people into releasing information (such as passwords) or performing actions that compromise confidential data, such as clicking on a link that enables someone else to remotely control a machine. In fact, the SANS Institute identifies phishing as one of the biggest Internet security risks.

For example, a spy might call the help desk from a pay-as-you-go mobile phone, claim to be working at home and request that a new username and password be sent as a text message to his phone. And some spies employ what the SANS Institute calls "spear phishing," in which they send individual employees highly targeted e-mail messages that include specific information designed to make the messages look genuine. For instance, a request for usernames and passwords might appear to be from the head of human resources.

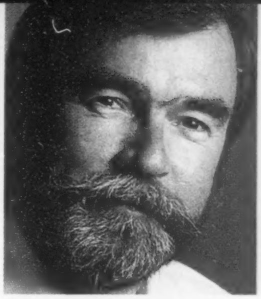
>>> How to stop them: Wood suggests training staffers to be cautious and giving them tips on how to detect social engineering. For instance, he says, they should withhold information when callers act rushed, drop names, use intimidation, ask odd questions or request forbidden information. There should also be clear policies as to how to report an incident and to whom.

The SANS Institute says it's important to continually raise employee awareness of these techniques, perhaps through drills that involve mock phishing attempts. Companies should also avoid exposing too much information on public Web sites, including logos and employee e-mail addresses. ■

Brandel *is a* Computerworld *contributing writer. You can contact her at marybrandel@verizon.net.*

SPOTLIGHT | OPINION

Mark Hall



Shhh! Privacy, Please

LIBRARIANS WILL go a long way to defend the privacy of their patrons' reading habits. How far will you go to defend the privacy of your customers' information and your employees' personal data?

In 2003, the chief librarian of the city of Santa Cruz, Calif., was able to warn her patrons about whether the FBI had served a National Security Letter (NSL) demanding information about who was reading what books. She managed that task despite specific provisions in the USA Patriot Act at the time that prohibited librarians or booksellers from revealing to anyone that they'd been issued an NSL.

So, how did the librarian get the word out? By regularly reporting to the library board that no NSL had been issued to any of the city's 10 branches, which was perfectly legal. Everyone knew that if the chief librarian failed to report that nothing had happened, then indeed an NSL had been served.

In 2005, Windsor, Conn.-based Library Connection Inc., which serves 27 Connecticut libraries, received an NSL and, instead of following its gag-order provisions, went to the American Civil Liberties Union and took the government to court. After a bit of legal threats and maneuvering, the next year, the government decided to stop defending the gag order.

"Protecting user privacy is an ethical obligation of librarians," says Deborah Caldwell-Stone, deputy director in the office of intellectual freedom for the American Library Association (ALA) in Chicago.

Cindy Hill, past president of the Special Libraries Association in Alexandria, Va., and now vice president of information management services at Outsell Inc., a market research firm in Burlingame, Calif., says virtually every librarian will comply with a court order or subpoena, where a specific suspect has been identified by law enforcement agencies.

CIOs can learn from librarians by establishing privacy audits of systems.

Leonard Kniffle, editor in chief of *ALA Magazine*, agrees, saying, "No librarian is not going to comply with a legal process."

But librarians also know where to draw the line. Both Hill and Kniffle say librarians will balk at what they consider "fishing expeditions," where the government simply wants to know who has been reading this or that book.

Let's face it: When it comes to keeping data secure, there's plenty that IT can learn from librarians. Just as ALA members ensure that their patrons' reading habits remain strictly private by establishing privacy audits, so, too, can CIOs audit their systems to ensure that customer and employee data is protected, says Caldwell-Stone. Privacy audits keep customer and employee content under wraps and can protect companies from embarrassing revelations.

One recent example of this was when news broke in February that employees of WE Energies in Milwaukee were accessing customer databases for personal use, such as checking up on their boyfriends.

But Hill says it goes beyond mere PR gaffes. CIOs for global companies need to take into account the privacy laws in different countries when designing IT systems. For example, what's legal for managers to glean about their employees differs from nation to nation, thus making HR applications, and the information they contain, cross-border regulatory land mines.

Hill cites an example from her past as a corporate librarian at Failure Analysis, a company that tested how and why technology failed. For one particular experiment, Hill says engineers needed to know specific physical traits about testers, such as their weight and foot size. Yet without explicit voluntary approval from the worker involved, just gathering, let alone storing, the information could violate worker privacy in more than one country.

Librarians have been trained to consider privacy ramifications surrounding access to content. They guard those rights vigorously and are a great example for CIOs designing secure systems. Just ask them. Quietly, of course. ■

Mark Hall *is a* Computerworld *editor at large. Contact him at mark_hall@computerworld.com.*

Career Watch

JUST BECAUSE THEY'RE **REMOTE,** IT DOESN'T MEAN THEY AREN'T **ENGAGED.**

Remote and home-based workers consistently were more likely to choose one of the two most positive answers (typically "strongly agree" or "agree") when presented with these statements:

SOURCE: KENEXA RESEARCH INSTITUTE'S 2007 WORKTRENDS SURVEY OF MORE THAN 10,000 U.S. WORKERS

	Office workers	Remote and home-based workers
I am not seriously considering leaving my company within 12 months.	46%	53.2%
Considering everything, I am satisfied with my company as a place to work.	63.6%	73%
I am proud to tell people I work for my company.	63.5%	70.4%
I have confidence in the future of my company.	63.8%	70.1%
I would gladly refer a friend.	55.4%	62.3%
My company supports employees' efforts to balance work and family/personal responsibilities.	56.7%	62.6%
Management shows concern for the well-being and morale of team members.	48.9%	56.2%
Senior management demonstrates that employees are important to the success of the company.	50.7%	58.2%
Senior management gives employees a clear picture of the direction the company is headed in.	48.6%	54.1%
When my company's senior management says something, you can believe it's true.	44.3%	52.5%
In my company, there is open, honest, two-way communication.	43.5%	53.9%
My manager does a good job at "people management."	56%	64.3%
My manager treats people fairly.	67.1%	73.8%
My manager gives me useful feedback on how well I'm doing my job.	60.4%	66.7%

PAGE COMPILED BY JAMIE ECKLE.

ASK A PREMIER 100 IT LEADER

Scott Penberthy

The chief technology officer at **Heavy Inc.** responds to questions, offering thoughts about trust and the issue of youth vs. experience.

What are the most important skills for an IT professional to have to advance his career? Be someone people can trust to get a job done – and done well. Trust is something that takes months and years to build, but seconds to destroy. Begin with the little things at work. If you say you're going to call, call. If you see someone in the hall and mention you'll send an e-mail, send it. When asked to get something done, ask what date they need it, then determine a day you can reasonably accomplish the task. If the date is unreasonable, say so and offer an alternative. Then deliver. Hit your date. Trust is not about being nice and agreeing to do everything as asked. In fact, it can mean getting in people's faces, when warranted, to figure out the right answer for your company. Bring bad news up quickly, and don't hide it. Your colleagues, boss, partners and customers will learn to trust that you'll do as you say. They'll see you can practice your art of IT in delivering a solid solution, in time. That lets them do *their* jobs reliably.

COMPUTERWORLD.COM

QUESTION?
If you have a question to pose to one of our Premier 100 IT Leaders, send it to askaleader@computerworld.com and watch for this column each month.

A year ago, I received a bachelor's degree in computer science, and now I am one semester away from getting an MBA. My problem is age. I am in my mid-50s, and I find there are very few, if any, companies willing to hire someone in my age group. The lone interview I have had was with a large utility company, and as I left, the HR representative commented that they were looking for someone younger with no corporate experience. Do I have a chance to re-enter the computer field, or am I doomed to shoveling concrete as I did after being discharged from the Navy many years ago? If you see yourself as doomed to shovel concrete, that's what you'll do. If you see people as reluctant to hire you because of your age, that's what you'll experience. We get what we expect.

Change your perspective. Focus on what you want to do, where you want to go. You offer what young college graduates cannot. You combine an experience rich with teamwork, organizational behavior, proven entrepreneurial drive, business management – all topped with the latest in computer science technology.

The HR person you met sounds like a loser. Don't let the losers pull you down. Instead, package all you have to offer, attack the opportunities with the vigor of youth, and expect to beat others hands down. Guess what – it works.

VoIP Network Specialist to work in McAllen, Texas. Install, configure and support Linux, Solaris and Windows servers, Cisco routers, switches and remote access servers. Install and maintain Voice over IP hardware and software. Submit resume to Juan Salazar at New Voice Telecom, LLC via e-mail jsalazar@newvoicetel.com. Put job code VNS001 on resume.

Thinc Systems, Inc seeks system analysts, s/w engineers, DBA, IT Managers to customize applications using Java, J2EE, .NET, Cognos, SAP, Oracle etc. Require MS or BS w/ exp. Travel required. Please contact bikki@thincsys.com. EOE

Soft O Soft (AdvanSoft) seek s/w engineer, system analyst, DBA to customize applications using Oracle, Java, VB, WebSphere, etc per project requirements. Candidate must have MS or BS with 1-5yr IT exp. Travel maybe required. Please email resumes to: info@softosoft.com

Computer/Technical: NJ Network & Computer Systems Administrator w/ Master's degree in Info. Sci., Comp. Sci., or related plus 2 yrs. exp. in job offered or related, including 1 yr. exp. in Analysis & Development of Computer apps; System Integration & Implementation; SQL &/or PL/SQL; Visual FoxPro; IT Project Management; & BarTender/Label Matrix. Resume: Fashion Logistics, Inc., 621 Route 46 West, Hasbrouck Heights, NJ 07604.

Computer IT - Other. Sogeti USA LLC, IT Consulting Co. HQ in Dayton, OH currently seeks IT professionals to fill Consultant positions located nationwide. Specific skill sets needed include:

- Web Development - Job #010 (send to Sogeti-job010@sogeti.net)
- Business Intelligence Consultants - Job #020 (send to Sogeti-job020@sogeti.net)
- Database Services - Job #030 (send to Sogeti-job030@sogeti.net)
- CRM Consultants - Job #040 (send to Sogeti-job040@sogeti.net)
- EAI Development - Job #050 (send to Sogeti-job050@sogeti.net)
- Testing & QA Analysts - Job #060 (send to Sogeti-job060@sogeti.net)
- Network Services - Job #070 (send to Sogeti-job070@sogeti.net)
- ERP Consultants - Job #080 (send to Sogeti-job080@sogeti.net)
- PLM Consultants - Job #090 (send to Sogeti-job090@sogeti.net)
- Mainframe Developers - Job #100 (send to Sogeti-job100@sogeti.net)
- Business Analysts - Job #110 (send to Sogeti-job110@sogeti.net)
- Project Managers - Job #120 (send to Sogeti-job120@sogeti.net)

FOR CONSIDERATION, YOU MUST (1) SEND EMAIL W/ RESUME TO EACH APPLICABLE EMAIL ADDRESS, AND (2) HAVE AUTHORITY TO WORK PERMANENTLY IN U.S. Entry through Sr. level positions available. Competitive salaries. Must be willing to travel/relocate.

Lead Applications Programmer/Analyst to act as dvlpr for integrated clinical applics. Dsgn, dvlp & support integration components following SDLC. Dvlp & support data analytical solutions & serve as primary tech'l contact for clients & coord dvlpmt activities w/vendors across the globe. Bachelor's in C.S. or rel. field or foreign equiv + 12 mos rel. exp in client/server s/ware dvlpmt & proficiency in C#.Net, VB.Net, .NET framework, PHP, MS SQL Server 2005/2000 (data access, stored procedure, triggers, indexing), SSIS, Reporting Services & Web Services, XML and object oriented prgmg. Send resumes to H.R. Manager, Whole Health Management, One Cleveland Center, 25th Fl, 1375 E. 9th St, Cleveland, OH 44114

Chevron seeks Product Analyst in San Ramon, CA. BS in Electrical/Computer Engineering, MIS or Computer Science + 5 yrs exp in job offered or as Software Delivery Specialist, Software Engineer or related. Reqd skills: project management & planning using MS Project Software; SQL servers & Windows Scripting; Windows 2000/2003 sever, SM & SCOM; ITSM and GIL Tools. Mail resume: Chevron, 1400 Smith St., Houston, TX 77002 attn Y. Vasquez. Ref job 81.

Director of Computer Information Systems: Light Sources, Inc. has an immediate opening for a Director of Computer Information Systems in Orange, Connecticut.

Duties: Responsible for managing all computer software/hardware maintenance, backup and development. Direct daily operations of IT department; manage backup, security and user help systems. Manage global websites. Evaluate technology use and needs and recommend improvements/upgrades. Meet with department heads, other managers and vendors to evaluate operations and resolve problems.

Requirements:
Bachelor's Degree in Computer Science, Computer Engineering or related field and five years of experience in software design, development, system analysis or related field.
Experience in application design and development working in MS-Server OS, MS-Exchange Mail Server, CRM application, Java, Java Script, Visual C, SQL, SWIP, Sage PRO, JDE, LabView, AutoCad, HTML, Perl, and LiveLink, website design and search engine optimization.

Please send resume and cover letter to:
Controller - AKH0206PA
Light Sources Inc.
37 Robinson Boulevard
Orange, CT 06447.

IT|careers

Searching for *diverse* IT Talent?

Let Computerworld IT careers put your recruitment message in front of over 1,400,000 qualified IT professionals!

Contact Laura Wilkinson for details at laura_wilkinson@itcareers.net or call 847.441.8877

SENIOR SYSTEMS ANALYST

Roseburg Forest Products has an opening for a Systems Analyst who will be primarily responsible for assessing all aspects of core business processes and procedures utilizing best business practices and current analysis techniques and methodologies. The Systems Analyst will also routinely perform as a cross-functional team member or leader to analyze business problems and define business requirements, and identify and recommend solutions to complex problems and enhancements to current procedures or processes. The Systems Analyst will work as a liaison between the business and the IT development teams identifying customer needs, translating those needs into workable business solutions, actively participating on process improvement teams and leading technical teams on medium to large size projects. Responsibilities include: Design, test, implement and maintain medium complexity software applications, queries and reports adhering to the standards documented within the IS department while working under little or no direct supervision; Effectively use case analysis, requirements analysis and process modeling in assessing processes and procedures; Meet policies and procedures for testing and promoting applications and reports; Write detailed application and report documentation following established guidelines; Conduct end user training programs and support; Manage large and small scale software implementation/business process reengineering projects.

Minimum Requirements: Master's degree in Information Systems or Computer Science plus two years of experience in a related field or, in the alternative, Bachelor's degree plus five years of progressive experience. Experience must include at least two years with JD Edwards Software/ERP implementation, architecture and/or development. All Candidates must have legal authority to permanently work in the US. Applicants meeting all requirements, please apply online at http://rfpcojobsa.iapplicants.com.

Roseburg Forest Products
Equal Opportunity Employer

SENIOR PROGRAMMER ANALYST

Roseburg Forest Products has an opening for a Senior Programmer Analyst who will be responsible for converting moderately complex application specifications into functional programs, queries or reports in JD Edwards EnterpriseOne ERP system and all other packaged and custom software applications. The Programmer Analyst will provide technical support for the applications, reports and/or interfaces, resolve technical issues of medium complexity utilizing the tools and resources available, assist business analysts in the design and preparation of functional specifications and also assist less experienced programmer analysts in all phases of application development and testing. Responsibilities include: Design, code, test, implement and maintain medium complexity software applications, queries and reports adhering to the standards documented within the IS Department while working under little or no direct supervision; Debug and resolve moderately complex technical problems; Meet policies and procedures for testing and promoting applications and reports; Write detailed application and report documentation following established guidelines; Conduct end user training programs and support.

Minimum Requirements: Master's Degree in Information Systems or Computer Science plus 2 years of experience in a related field or - in the alternative - Bachelor's Degree plus 5 years of progressive experience. Experience must include 2 years in JD Edwards Software/ERP implementation, architecture and/or development. All Candidates must have legal authority to permanently work in the US. Applicants meeting all requirements, please apply online at http://rfpcojobsa.iapplicants.com.

Roseburg Forest Products
Equal Opportunity Employer

SAP Exchange Infrastructure Solution Consultant (Atlanta, GA) Provide sales business and technical consulting for Seeburgers' XI electronic commerce solutions. Requires a Bachelor's degree or foreign degree equivalent in Computer Information Systems or a closely related field plus 2 years of experience in the job offered or as a Solution Architect. Send resumes to: Controller, Seeburger Inc. 1230 Peachtree Street, N.E., Suite 1020, Atlanta, GA 30309. (No Phone Calls)

Law Crossing, Inc. located in Pasadena, CA seeks a Programmer Analyst. Reqs Bachelors in Comp Sci or equiv based on any combo of education and/or exp, and 2 yrs exp in programming, sys analysis, & tech support. Mail resumes to Judy Streppone, HR Mgr at 175 S. Lake Ave, # 200, Pasadena, CA 91101 or fax resumes to 213-895-7306

SharkTank

TRUE TALES OF IT LIFE AS TOLD TO SHARKY

Just One Thing

Consultant pilot fish gets a panicked call from a client: "Everything was working fine. We went into a meeting, and when we came out, nothing worked. We couldn't access the Internet or the server, or use our VoIP phones." Fish arrives on-site; the network is completely down, so he starts testing. As client watches fish connecting his laptop directly to the router, he comments, "Oh yeah, I did do something in the conference room. I connected a wire to a jack." A little digging turns up the rest of the story: Going into the conference room for the meeting, the client noticed an unconnected network cable. It's for an iMac that's been moved to another room, but client decided the logical place to plug in the cable was an unused network port on the back of the VoIP phone. "Not only did it create a loop in the data network, it looped the voice switch to the data switch," sighs fish. "I just loved his 'Oh yeah, I did do one thing.' "

Sure There's a Reason: It Won't Work

Trouble ticket comes to this pilot fish at a university computing center: "There is a problem with the code used in changing passwords. The password standard states: 'Password Composition and Complexity: At least one numeric that is not at the end or the beginning of the password.' I attempted to change my password to one that had an internal number *and* a number at the end. I got the following error message: 'Error: Could not complete request. Password may not end with a number.' There is no reason not to end a password with a number so long as there is also an internal number. This appears to be an error in translating the standard into code."

Aha!

Support pilot fish investigates a user's problem: She has dual screens and complains that the mouse won't move between them. "User has a laptop with an external monitor," fish reports. "Both screens showed the lovely tulip wallpaper she had selected, so the video card was set to extended desktop. But when I tried to go from the laptop to the external monitor, the mouse stopped at the edge of the laptop's screen. Then the user said, 'I don't understand why it suddenly stopped working. All I did was put the monitor over on the other side.' Straight-faced, I moved the mouse away from the 'stuck' edge and continued to the right. The mouse icon magically went off the screen, all the way around the world, and showed up on the 'left' screen's left edge. Apparently, the user thought the laptop would know she moved her monitor to the other side."

■ *Sharky knows you've got a true tale of IT life to tell. Move it in my direction: sharky@computerworld.com. You'll score a sharp Shark shirt if I use it.*

COMPUTERWORLD.COM

TIRED OF BUNGLING BOSSES and clueless co-workers? Swim on over to Shark Bait and share your tales of woe: **sharkbait.computerworld.com**.

CHECK OUT Sharky's blog, browse the Sharkives and sign up for Shark Tank home delivery at **computerworld.com/sharky**.

■ COMPANIES IN THIS ISSUE

Page number refers to page on which story begins. Company names can also be searched at computerworld.com

Adobe Systems Inc. 19
Advanced Micro Devices Inc. 10, 12, 14
Airline Reporting Corp. 17
ALA Magazine 39
Algorithmic Security Inc. 32, 33
American Civil Liberties Union 39
American Library Association. 39
Apple Inc. 14
AppStream Inc. 12
Aria Systems LLC 19
Asero Worldwide Inc. 33
Asustek Computer Inc. 14, 24
AutoZone Inc. 10
Best Buy Co. 10
BitTornado 32
Case Western Reserve University 8
Check Point Software Technologies Inc. 30
Computer Sciences Corp. 36
Control Risks Group Ltd. 32, 33
Datomics Licensing 14
Deloitte & Touche LLP 28, 30
eBay Inc. 30, 33
EffectiveUI Inc. 19
EMC Corp. 14
eMule 32
Facebook Inc. 22, 32
Failure Analysis Associates Inc. 39
FBI. 39
Fenwick & West LLP 35
FilesX Inc. 12
First Base Technologies 36
Gartner Inc. 12, 16, 18
General Datomics 14
Georgetown University 8
Google Inc. 20, 32
Hannaford Bros. Co. 16
Heavy Inc. 40
Hotmail. 32
IBM 12, 14, 30
IDC 10
Intel Corp. 10
International Information
Systems Security
Certification Consortium Inc. 26, 28, 30
Internet Security Advisors Group. 36
Internet Security Systems Inc. 30
Iomega Corp. 14
iSec Partners Inc. 32
JupiterResearch 24
Kazaa 32
Kenexa Research Institute. 40
Library Connection Inc. 39
Lumension Security Inc. 17
MGM Mirage. 18
Microsoft Corp. 10, 14, 19,
.... 20, 22, 24, 30
Midwest Cooperative Education
and Internship Association 8
MokaFive Inc. 19
Monsanto Co. 8
MySpace.com 22, 32
MySQL AB 10
NetWitness Corp. 17
Network Risk Management LLC 26
Okemo Mountain Resort. 16
Oracle Corp. 10, 12
Outsell Inc. 39
Ovum Ltd. 14
Providence Health and Services 34
SANS Institute. 36
Shavlik Technologies LLC 14
Soy Capital Bank and Trust Co. 14
Special Libraries Association 39
Starbucks Corp. 34
Stiefel Laboratories Inc. 10
Storage Networking Industry Association 10
SunGard Data Systems Inc. 19
Symantec Corp. 12
SystemExperts Corp. 28, 30
Tamiyasu, Smith, Horn and Braun
Accountancy Corp. 14
Tensa Kft. 14
The Aerospace Corp. 10
The Benchmark Group 34, 35
Top Layer Networks Inc. 17
U.S. Citizenship and
Immigration Services 10
U.S. Department of Homeland Security. 10
U.S. International Trade Commission 14
U.S. National Reconnaissance Office 34
University of Illinois 12
University of Nebraska 28
Urban Institute. 8
VeriFone Inc. 17
Vertafore Inc. 34, 35
WE Energies. 39
Yahoo Inc. 14, 32
YouTube Inc. 22, 32

[illegible]

Akamai C3
www.akamai.com/10years
BigFix 25
www.bigfix.com/geteyes
Canon. 4-5
www.usa.canon.com
CDW Corporation. 23
CDW.com
Hewlett-Packard ProLiant. 15
hp.com/go/dependable14
Hewlett-Packard Software C4
hp.com/go/servicemanagement
IBM IT Campaign 7, 29, 31
ibm.com
InterSystems. 3
InterSystems.com/Cache26A
Juniper Networks. 13*
www.juniper.net/federal
Juniper Networks. 13*
www.juniper.net/connected
Kodak 35
kodak.com/go/galeforce
Microsoft Forefront C2-1
easyeasier.com
Novell 21
www.moreinterop.com
SAS. 11
www.sas.com/giraffes
SonicWALL. 37
www.sonicwall.com/dandelion
Storage Networking World 43
www.snwusa.com

* Regional Select

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

Periodical postage paid at Framingham, Mass., and other mailing offices. Posted under Canadian International Publication agreement PM40063731. **CANADIAN POSTMASTER:** Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A 7C9. Computerworld (ISSN 0010-4841) is published weekly: except for a single combined issue the first two weeks of July and the last two weeks of December by Computerworld, Inc., 1 Speen Street, Box 9171, Framingham, Mass. 01701-9171. Copyright 2008 by Computerworld Inc. All rights reserved. Computerworld can be purchased on microfilm and microfiche through University Microfilms Inc., 300 N. Zeeb Road, Ann Arbor, Mich. 48106. Computerworld is indexed. Back issues, if available, may be purchased from the circulation department. Photocopy rights: permission to photocopy for internal or personal use is granted by Computerworld Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of $3 per copy of the article, plus 50 cents per page, is paid directly to Copyright Clearance Center, 27 Congress St., Salem, Mass. 01970. Reprints (minimum 100 copies) and permission to reprint may be purchased from Erik Eberz, Computerworld Reprints, c/o The YGS Group, Greenfield Corporate Center, 1808 Colonial Village Lane, Lancaster, Pa., 17601, (800) 290-5460, Ext. 150. Fax: (717) 399-8900. Web site: www.reprintbuyer.com. E-mail: computerworld@theygsgroup.com. Requests for missing issues will be honored only if received within 60 days of issue date. Subscription rates: $5 per copy: U.S. – $99.99 per year; Canada – $130 per year; Central & So. America. $250 per year; Europe – $295 per year; all other countries – $295 per year. Subscriptions call toll-free (888) 559-7327. **POSTMASTER:** Send Form 3579 (Change of Address) to Computerworld, PO Box 3500, Northbrook, Ill. 60065-3500.

COMPUTERWORLD SNIA
STORAGE NETWORKING WORLD

Best Practices IN STORAGE

AWARDS PROGRAM

AWARDS PROGRAM EXCLUSIVELY SPONSORED BY:

HITACHI
Inspire the Next

Congratulations Award Recipients!

Storage Networking World proudly announced the results of the "Best Practices in Storage" Awards Program. This program honors IT users "Best Practice" case studies selected from a field of qualified finalists.

Honoree Award Recipients in each of the following categories were recognized during the Gala Awards ceremony at Storage Networking World in Orlando, Florida, on April 9th:

Innovation and Promise

Livermore Computing, Livermore, California

Finalists:
- Fleet Management Limited, Wanchai, Hong Kong
- Sprint Nextel, Overland Park, Kansas
- Tucson Electric Power, Tucson, Arizona
- University of North Texas, Denton, Texas

Planning, Designing and Building a Strategic Storage Infrastructure

British Columbia Interior Health Authority, Kelowna, British Columbia

Finalists:
- 3ality Digital, Burbank, California
- General Motors Corporation, Warren, Michigan
- Infosys Technologies Limited, Bangalore, India
- VaultLogix, LLC, Ipswich, Massachusetts

Selecting and Deploying Storage Networks

NASCAR Media Group, a full-service production company and broadcast division of NASCAR, Charlotte, North Carolina

Finalists:
- ICICI Bank Limited, Mumbai, India
- Microsoft Studios, Redmond, Washington
- Rockford Construction Company, Inc., Grand Rapids, Michigan
- The University of Maryland, College Park, Maryland

Storage Reliability and Data Recovery

New York Independent System Operator, Rensselaer, New York

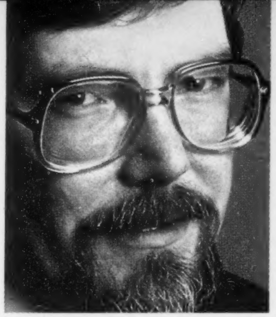
Finalists:
- Gaston County, Gastonia, North Carolina
- Management Council - Ohio Education Computer Network, Archbold, Ohio
- Safeguard Properties, LLC, Brooklyn Heights, Ohio
- Tucson Electric Power, Tucson, Arizona

Thank you to our "Best Practices in Storage" Judges for SNW Spring 2008:

- Peter Amstutz, Defense Contract Management
- Andres Carvallo, Austin Energy
- Scott Dennull, CareSoure
- Brian Fonseca, *Computerworld*
- Dale Frantz, Auto Warehousing Company
- Noemi Greyzdorf, IDC
- Julia King, *Computerworld*
- William Kramer, NERSC
- Richie Lary, Lary.com
- Lucas Mearian, *Computerworld*
- Ron Milton, *Computerworld*
- Mark O'Gara, Highmark, Inc.
- Arun Taneja, Taneja Group
- Mark Showers, Monsanto Company
- Jim Swartz, Sybase, Inc.
- John Webster, Illuminata, Inc.
- Ben Woo, IDC

FRANKLY SPEAKING

Frank Hayes



Security Team

HOW MANY people do you have working to protect your data, systems and networks? Go ahead, count 'em up. We'll wait. Finished? Here's the bad news: Unless you've just counted every person in your organization — not your IT department, but your entire enterprise — it's not enough.

You need them all. Every secretary and salesman. Every receptionist and researcher. Every executive and engineer. Every manager and maintenance guy. You need them all on board. You need every one of them looking out for the information that's critical to your business.

Do they have to be security experts? Of course not. You have an IT security team for that.

But that's not enough.

Look, we've all inherited our ideas about IT security from a simpler time. The data was in the glass house. We guarded it. Simple, no?

No. It wasn't that simple. It wasn't enough then, either. Information was all over the organization, in reports and notebooks, filing cabinets and desk drawers. Crooks and spies and hackers wormed their way in and walked away with critical information, even if they never got near the data center. Occasionally, we caught them in time. Usually we just learned about it later. Often, we never found out at all.

The IT security team wasn't enough then. It's certainly not enough now.

That's OK. You can get everyone else working for IT security too.

But it's going to require some changes.

First, you've got to understand that IT security pros aren't enough.

Then you've got to understand that the rest of your organization isn't the enemy.

Your fellow employees may be a security problem, but they're not intent on destroying their jobs. Not most of them, anyhow. They're only a problem because they think IT security means a collection of annoying rules telling them they can't open a picture of Aunt Margie attached to an e-mail message.

All employees have a part to play – a major part, one that in aggregate dwarfs what the IT security pros can do.

That's the wrong end of the telescope. IT security is about protecting critical company assets, the information that's the lifeblood of the enterprise: customer data, financial information — everything that helps make the company successful and competitive.

It's in every employee's interest to protect those assets — every employee except for the few crooks, spies and hackers on the inside.

And except for those internal threats, it's not hard to get people to understand that IT security is in their interest. And that they have a part to play — a major part, one that in aggregate dwarfs what the IT security pros can do.

They know how things are supposed to work. They know what looks a little odd. They know what rules will always be bent, what corners will always be cut. And they represent hundreds or thousands of eyes and ears and brains that can filter out the ordinary business and help spot the real threats.

With a little support from you, a little explanation, a little training, they'll do it. They'll be glad to. Not because it's in their job descriptions, but because it's in their interest.

That's the easy part.

The hard part? It's for your IT security people to adjust to this strange new world in which thousands of employee eyes, ears and brains help them do their jobs.

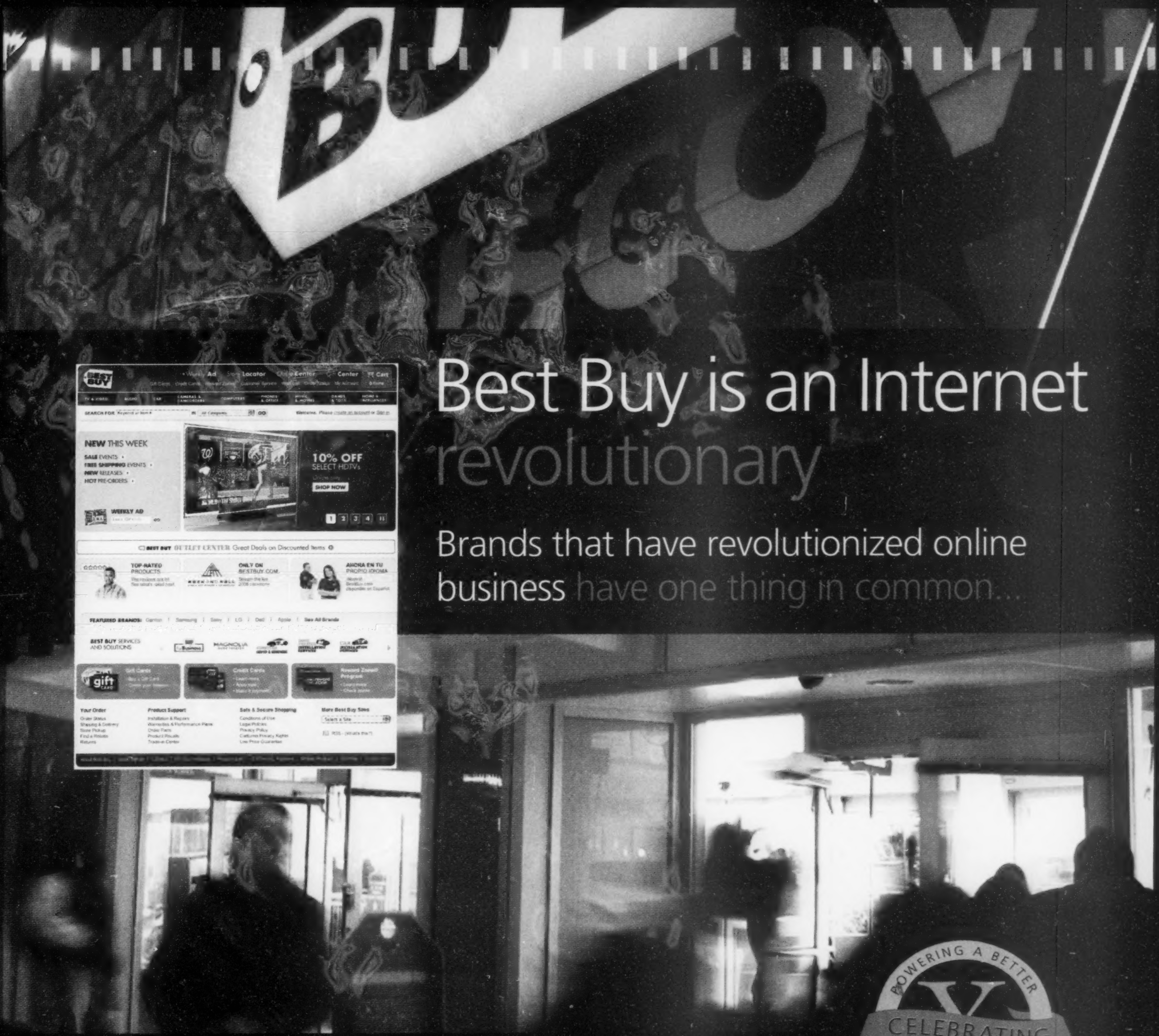
But they can do that. It's in their interest, too.

The threats are out there — in greater numbers, with more sophistication and variety, and delivering orders of magnitude more attacks against you. To beat them, you need all the help you can get.

You need the help of everyone in your organization.

And that's something you can count on. ■

Frank Hayes *is* Computerworld*'s senior news columnist. Contact him at frank_hayes@computerworld.com.*



Best Buy is an Internet revolutionary

Brands that have revolutionized online business have one thing in common…

POWERING A BETTER INTERNET SINCE 1998
CELEBRATING X YEARS

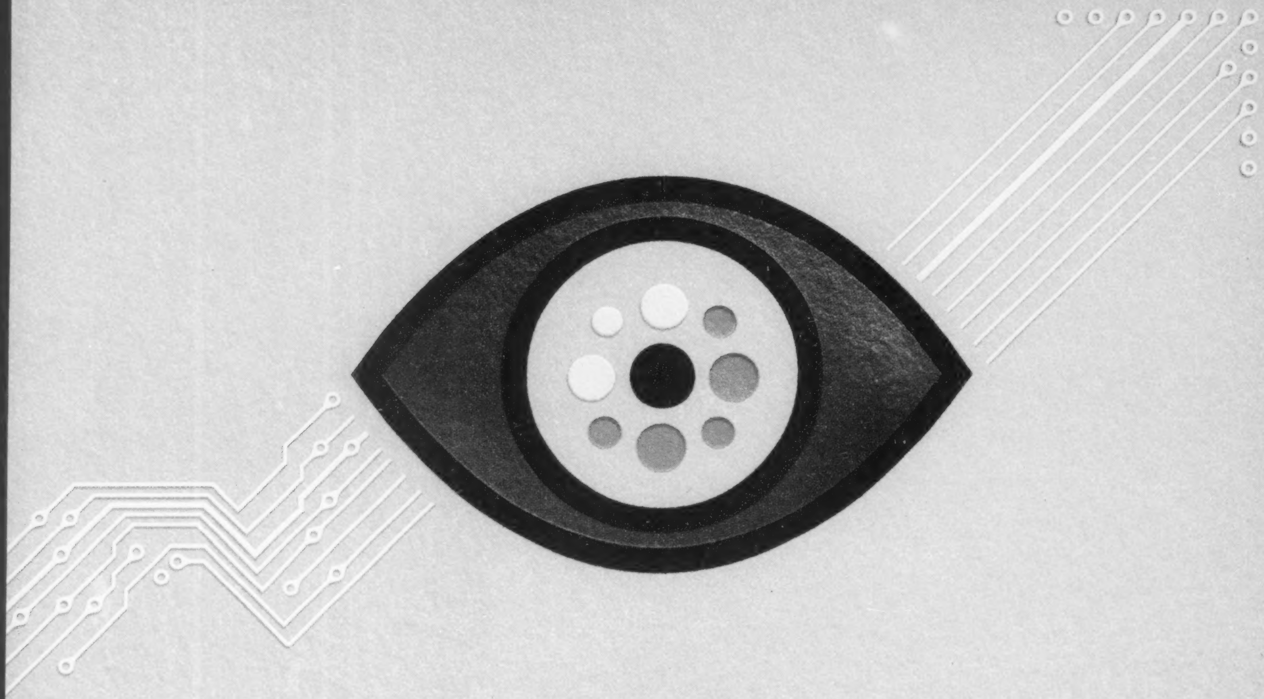
…Akamai, Enabling the Revolution

Best Buy has been ranked number one for handling daily Web site volume during the holidays. Having added mashups, waiting room applications, and customer-powered content, Best Buy has revolutionized its online customer experience by integrating interactive and rich media, and providing a personalized shopping environment.

A lot can happen in ten years. Especially with Internet technology that's revolutionizing virtually every facet of business. New sales channels. New applications and business processes. New opportunities—and risks. In our first ten years, Akamai has helped the world's leading businesses become the world's leading online businesses. And we're just getting started.

Learn more at www.akamai.com/10years

Akamai



ALTERNATIVE THINKING ABOUT SERVICE MANAGEMENT:
Business Driven. Not Just Business Aligned.

Alternative thinking is repositioning IT from the server closet to the front lines, embracing its impact on the business (not just in a PowerPoint® deck, but actually doing it).

It's rewiring the rules of engagement to identify problems, prioritize solutions and automate change (before things become business critical).

It's partnering with HP, a pioneering force behind ITIL, to leverage the experience of certified consultants and utilize the ingenuity engrained in the DNA of our software.

It's placing business metrics under the microscope every day, every minute, every nanosecond—enhancing insight and extending control (from a financial perspective, for a change).

Technology for better business outcomes. hp.com/go/servicemanagement

hp

©2008 Hewlett-Packard Development Company, L.P. PowerPoint is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.